VYSOKÁ ŠKOLA BÁŇSKÁ – TECHNICKÁ UNIVERZITA OSTRAVA

EKONOMICKÁ FAKULTA

KATEDRA SYSTÉMOVÉHO INŽENÝRSTVÍ

Návrh procesu implementace GDPR ve školství
Design of a GDPR Implementation Process in Education

Student: Bc. Anna Vaňková

Vedoucí diplomové práce: Mgr. Ing. Lucie Chytilová, Ph.D.

Ostrava 2019

VŠB - Technická univerzita Ostrava
Ekonomická fakulta
Katedra systémového inženýrství

Zadání diplomové práce

Student: **Bc. Anna Vaňková**

Studijní program: N6209 Systémové inženýrství a informatika

Studijní obor: 6209T017 Informatika v ekonomice

Téma: Návrh procesu implementace GDPR ve školství
Design of a GDPR Implementation Process in Education

Jazyk vypracování: čeština

Zásady pro vypracování:

1.Úvod
2.Teoretické vymezení projektového managementu a právního rámce GDPR
3.Metodická východiska řízení projektů
4.Analýza současného stavu a požadavků GDPR
5.Návrh procesu implementace GDPR ve školství
6.Závěr
Seznam použité literatury
Seznam zkratek
Prohlášení o využití výsledků diplomové práce
Seznam příloh
Přílohy

Seznam doporučené odborné literatury:

NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2017. Právo pro praxi. ISBN 978-80-271-0668-4.
NULÍČEK, Michal a kol. *GDPR - obecné nařízení o ochraně osobních údajů*. 2. vydání. Praha: Wolters Kluwer, 2018. ISBN 978-80-7598-068-7.
Project Management Institue. *A guide to the project management body of knowledge (PMBOK guide)*. Fifth edition. Newtown Square, Pennsylvania: Project Management Institute, 2013. ISBN 978-1-935589-67-9.

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **Mgr. Ing. Lucie Chytilová, Ph.D.**

Datum zadání: 23.11.2018
Datum odevzdání: 26.04.2019

doc. Ing. Jana Hančlová, CSc.
vedoucí katedry

prof. Dr. Ing. Zdeněk Zmeškal
děkan fakulty

Ráda bych poděkovala paní Mgr. Ing. Lucii Chytilové, Ph.D. za cenné rady, připomínky a čas, který mi věnovala při vedení mé práce. Dále děkuji panu Bc. Pavlu Říhovi za jeho odborné rady, zkušenosti, nápady a údaje, které mi poskytnul pro vypracování diplomové práce. V neposlední řadě, patří mé poděkování také mé rodině a všem blízkým za podporu během celého studia.

Prohlašuji, že jsem celou práci vypracovala samostatně. Přílohy č. 3, dané mi k dispozici, jsem samostatně doplnila, ostatní přílohy jsem vypracovala samostatně.

V Ostravě dne 23. 4. 2019

Vaňková

……

Bc. Anna Vaňková

Obsah

1 Úvod

Je to již téměř rok, co vešlo v platnost Obecné nařízení o ochraně osobních údajů (GDPR) vydané Evropskou unií za účelem sjednocení a modernizace právního řádu týkajícího se ochrany osobních údajů v zemích EU. Toto nařízení vyvolalo ve společnosti velký rozruch, a to především kvůli stanovení vysoké horní hranice pokut za porušení pravidel GDPR. Z toho důvodu by se mohlo zdát, že všechny organizace již mají požadavky GDPR implementovány a zpracování osobních údajů probíhá plně v souladu s tímto nařízením. Opak je však pravdou. Existuje mnoho organizací, které se sice problematikou implementace požadavků GDPR zaobíraly, avšak nezohlednily všechny nutné oblasti implementace, nebyly dostatečně důsledné, či si některou z oblastí špatně vyložily. K těmto případům dochází hlavně v situacích, kdy se organizace rozhodnou vzít implementaci požadavků GDPR zcela do vlastních rukou, bez zapojení odborníka, který se na tuto oblast specializuje. V dalších případech se organizace mnohdy mylně domnívají, že jakmile mají požadavky GDPR implementovány, již se nemusí touto oblastí dále více zaobírat.

Tématem diplomové práce je návrh procesu implementace požadavků nařízení GDPR ve školských organizacích. Součástí této práce je zmapováni požadavků Obecného nařízení o ochraně osobních údajů v prostředí školských organizací a navržení způsobu vypracování jednotlivých dokumentů s tímto nařízením souvisejících. Práce je vypracována na základě podnětu soukromého gymnázia, které se začalo zabývat problematikou GDPR v souvislosti s požadavkem na zavedení kamerového systému ve škole. K návrhu implementace GDPR jsou využity metody projektového řízení, čímž se minimalizuje riziko vzniku chaotických situací.

Cílem diplomové práce je navržení nezbytných kroků správné implementace požadavků GDPR spojených se zavedením kamerového systému ve škole Gymnázium BESKYDY MOUNTAIN ACADEMY, s.r.o. Dílčím cílem práce je navržení obecných kroků prvotní implementace požadavků GDPR ve školských organizacích, které se doposud tímto problémem nezabývaly.

Práce je rozdělena do několika hlavních kapitol. V teoretické části práce je řešena oblast projektového managementu, hlavní pojmy z této oblasti a rozbor základních přístupů a standardů. Dále je teoretická část zaměřená na Obecné nařízení a jeho základní vysvětlované pojmy, povinnosti, práva a sankce.

Další kapitola je zaměřena na hlavní metody využívané v projektovém řízení, jako je například Studie proveditelnosti, Metoda kritické cesty nebo Ganttův diagram.

Ve čtvrté kapitole práce je zmapováno prostředí soukromého gymnázia a jsou popsány základní kroky implementace pro dodržení požadavků GDPR.

V praktické části práce jsou jednotlivé kroky správné implementace podrobně rozebrány a jsou navrženy nezbytné postupy a metody takovéto implementace. Je zde vypracována studie proveditelnosti projektu implementace GDPR v souvislosti se zavedením kamerového systému, a také jsou připraveny další nezbytné dokumenty.

2 Teoretické vymezení projektového managementu a právního rámce GDPR

Tato kapitola je ve své první části zaměřena na oblast projektového managementu. Nejprve jsou zběžně vysvětleny nejčastější pojmy a principy vyskytující se v této oblasti a následně je zaměřena pozornost na hlavní přístupy a standardy zabývající se projektovým managementem. Druhá část kapitoly je věnována problematice GDPR. Jsou zde zmíněny hlavní oblasti a problémy řešené v rámci Obecného nařízení na ochranu osobních údajů vydaného Evropskou unií.

2.1 Projektový management

Každá organizace musí v rámci systému řízení provádět v čase jisté změny, které jsou více či méně zásadní. Řízení těchto změn se nejčastěji provádí pomocí projektů.

Pojem projektový management lze považovat za jakousi filozofii řízení projektu za pomoci definování předmětu projektu s jasně stanoveným cílem, kterého musí být dosaženo v daném časovém úseku, v předem dané kvalitě a při omezených nákladech. Od běžného řízení se projektový management liší především svou dočasností (Němec, 2002).

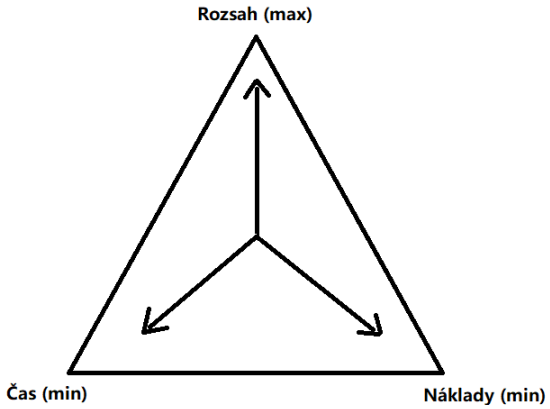
2.1.1 Projekt

Nejdůležitějším pojmem, který se v této oblasti vyskytuje je pojem *projekt*. Vokál (2013) definuje projekt jako soubor činností, aktivit a úkolů, které jsou jedinečné, mají jasně daný specifický cíl a jsou dokončeny v předem určeném čase a rozsahu.

Téměř každý autor zabývající se projektovým managementem má svou vlastní verzi definice projektu, avšak všichni se shodují na jeho základních charakteristických znacích. Základními charakteristikami projektu jsou:

- jedinečnost,
- vymezenost v čase, penězích a zdrojích,
- realizace projektovým týmem lidí z různých oborů,
- složitost a komplexnost,
- rizikovost.

U každého projektu můžeme pozorovat tři limitující faktory, kterými je projekt omezen. Jsou to náklady, čas a rozsah. Tyto faktory se vzájemně velmi ovlivňují a bývají v projektovém managementu nazývány projektovým trojimperativem. Úkolem projektového manažera je najít mezi časem, náklady a rozsahem projektu ideální poměr a vzájemně je sladit (Rosenau, 2007).



Obrázek 2.1 Trojimperativ (zdroj: vlastní zpracování)

Dalším společným faktorem všech projektů je životní cyklus projektu. Životní cyklus projektu, rozděluje projekt do několika fází od jeho zahájení až po úplné dokončení. Existuje mnoho různých způsobů, jak na životní cyklus nahlížet a jak jej dělit. Často využívané je jednoduché rozdělení projektu na část předprojektovou, projektovou a poprojektovou (Bendová, 2012).

Project Management Institute (2013) uvádí obecný životní cyklus projektu, který může být využitý na každý větší či menší projekt. Obecný životní cyklus podle Project Management Institutu má čtyři fáze a to:

- zahájení projektu,
- organizace a příprava,
- zajišťování projektových prací,
- ukončení projektu.

2.1.2 Přístupy a standardy řízení projektů

Standardy projektového řízení, na rozdíl od mnoha jiných oblastí jejichž standardy jsou čistě teoretické či technické, vychází z praktických zkušeností projektových manažerů a jsou jakýmsi souborem jejich nejlepších postřehů, nápadů a rad v oblasti řízení projektů. Z toho také vyplývá, že je nutné tyto standardy považovat spíše za doporučení a inspiraci nežli za zákon, který je nutné stoprocentně dodržovat. Asi největším přínosem standardů v projektovém řízení je sjednocení metod a terminologií, díky čemuž si lidé pracující na projektech jednoduše porozumí a jsou schopni snadněji spolupracovat.

Mezi hlavní a také nejznámějšími světové standardy patří PM BoK, PRINCE2, ICB a ISO 21 500. Vzájemně se liší hlavně v úhlu pohledu na věc, ve způsobu zpracování, a také organizací, která je zpracovala (Doležal, 2016).

2.1.3 PM BoK

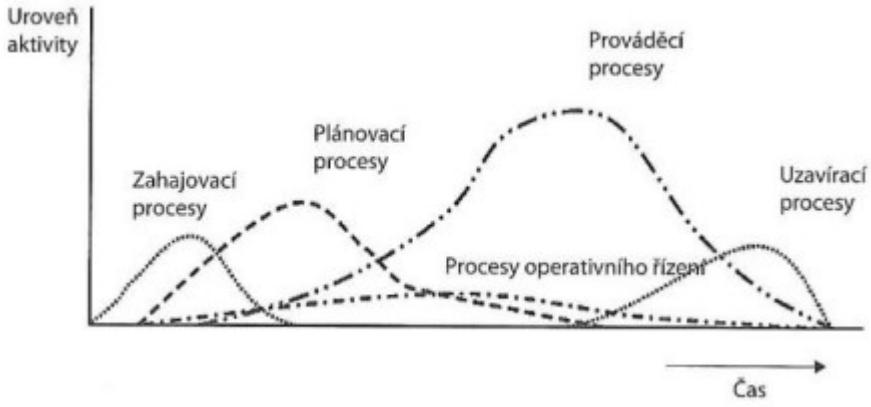
Jedná se o standard vytvořený institutem PMI (Project Management Institute). Celý jeho název je Project Management Body of Knowledge, byl vytvořen v roce 1986 a v současné době je dostupný ve svém šestém vydání.

PMI pohlíží na projektové řízení jako na soubor procesů, které se navzájem prolínají, překrývají a doplňují. Ve standardu je definováno čtyřicet sedm procesů, pět základních skupin procesů a deset oblastních znalostí (Doležal, 2016).

Skupiny, do nichž jsou procesy rozděleny jsou následující (Řeháček, 2013):

- procesy zahajovací,
- procesy plánovací,
- procesy prováděcí,
- procesy operativního řízení,
- procesy uzavírací.

Překrývání a navazování procesů neprobíhá pouze uvnitř těchto skupin, ale také mezi nimi, jak lze vidět na obrázku 2.1.



Obrázek 2.2 Překrývání procesů v projektu (zdroj: Řeháček, 2013)

Řeháček (2013) uvádí, že všechny procesy je možné popsat pomocí jejich vstupů, nástrojů a technik a výstupů, pomocí nichž jsou vzájemně propojeny.

PM BoK dále definuje deset oblastí znalostí, které obsahují procesy, činnosti a pojmy důležité pro danou oblast. Znalostní oblasti podle PM BoK jsou (Project Management Institute, 2013):

- řízení integrace projektu,
- řízení rozsahu projektu,
- řízení času projektu,
- řízení nákladů projektu,
- řízení kvality projektu,
- řízení lidských zdrojů projektu,
- řízení komunikace projektu,
- řízení rizik projektu,
- řízení obstarávání projektu,
- řízení zainteresovaných stran projektu.

Procesy, které jsou v tomto standardu popisovány, mohou být využívány opakovaně, avšak některé z nich také nemusí být použity vůbec, vše záleží pouze na konkrétním projektu a projektovém manažerovi.

Project Management Institute nabízí projektovým manažerům možnost certifikace, kterou nabízí v současnosti na osmi úrovních, pro různě zkušené odborníky (Česká komora PMI, 2019):

- Project Management Professional (PMP),
- Certified Associate in Project Management (CAPM),
- Program Management Professional (PgMP)
- Portfolio Management Professional (PfMP),
- PMI Agile Certified Practitioner (PMI-ACP),
- PMI Professional in Business Analysis (PMI-PBA),
- PMI Risk Management Professional (PMI-RMP),
- PMI Scheduling Professional (PMI-SP).

Principy projektového řízení vycházející ze standardu PM BoK jsou také dále využívány v této diplomové práci.

2.1.4 PRINCE2

Tento standard by původně vytvořen ve Velké Británii pro vládní projekty z oblasti informačních a komunikačních technologií. Postupem času byl přetvářen do obecnější a přizpůsobivější formy, tak aby jej bylo možno využít pro co největší škálu projektů z různých oblastí. Mnoho zdrojů uvádí, že v dnešních dnech se jedná o vůbec nejrozšířenější metodiku projektového řízení. PRINCE2 neboli PRojects IN Controlled Environments vlastní, spravuje a udržuje společnost Axelos. Základním prvkem PRINCE2 je sedm principů, témat a procesů, které je nutné dodržet, jestliže chceme tuto metodiku správně aplikovat (Doležal, 2016).

Principy, z nichž metodika vychází, jsou následující (BESTPACTICE.CZ, 2019):

- Neustála zdůvodnitelnost projektu – ve všech fázích projektu musí být jasný smysl projektu, a to po stránce obchodní i praktické.
- Učení se ze zkušeností – velikou pomocí při řízení projektu mohou být již nabyté zkušenosti z minulých projektů nebo z minulých fází právě

probíhajícího projektu a dobrý projektový manažer by měl být schopen těchto zkušeností využít k neustálému zlepšování sebe i celého projektu.

- Definování rolí a odpovědností – každý člověk v projektovém týmu musí vědět co má dělat, za co je odpovědný a co dělají ostatní členové týmu.
- Řízení pomocí etap – projekt by měl být naplánován jen rámcově, měl by být rozdělený na etapy a detailně naplánovaná a řízená by měla být jen aktuální etapa, v níž se projekt nachází. Tímto dochází ke zlepšení schopnosti reagovat na změny v projektu.
- Řízení pomocí výjimek – projekt má mít jasně stanoveny rezervy a míry tolerance, a zároveň jasně rozděleny odpovědnosti, aby každý věděl, co má dělat, když nastane výjimečná situace.
- Zaměření na produkty – projekt má být zaměřen hlavně na produkty, které mají být dodány a postupy, dokumentace atd., jsou pouze nástrojem k dosažení těchto produktů.
- Přizpůsobení se prostředí – metodiku je nutné si vždy upravit tak, aby seděla konkrétnímu projektu a jeho potřebám.

Vedle těchto principů jsou v metodice vyjmenována témata, která by měla být v rámci projektu aplikována a musí jim být věnována určitá pozornost. Jedná se o zdůvodnění projektu, organizaci, kvalitu, plány, rizika, změny a progres (BESTPACTICE.CZ, 2019).

Posledním důležitým okruhem, kterým se PRINCE2 zabývá, jsou procesy, které obvykle v rámci projektů probíhají. Jedná se o následujících sedm procesů (BESTPACTICE.CZ, 2019):

- zahájení projektu,
- řízení projektu,
- nastavení projektu,
- řízení etapy projektu,
- řízení dodávky produktu,
- řízení přechodu mezi etapami,
- ukončení projektu.

Projektoví manažeři mohou také získat certifikaci podle PRINCE2 ve čtyřech úrovních – PRINCE® Practitioner, PRINCE2® Foundation, PRINCE2® Agile a PRINCE2® Professional (Doležal, 2016).

2.1.5 ICB

Na rozdíl od předchozích dvou standardů, které jsou založeny na procesech, je tento standard založen na kompetencích projektových manažerů a členů projektových týmů. Vytváří jej a spravuje organizace IPMA (International Project Management Assotiation). Zároveň se jedná o nejstarší ze standardů, což může být důvodem odlišného pojetí řízení projektů. Celý název standardu je IPMA Competence Baseline.

Ve standardu je projektové řízení rozděleno do tří kompetenčních oblastí, kterými jsou kompetence technické, behaviorální a kontextové. Místo definování procesů, které by měly být při řízení projektů využívány, jsou v ICB pouze doporučeny jisté procesní kroky, které mohou být aplikovány konkrétními osobami.

Odlišnost standardu je také v tom, že organizace IPMA sdružuje národní organizace z celého světa, který ICB dále rozpracovávají, a tak vznikají národní standardy označované jako NCB (National Competence Baselines). Organizace IPMA působící v České Republice nese název Společnost pro projektové řízení, o. s. (Doležal, 2016).

Doležal (2016) uvádí certifikace, kterých je možné dosáhnout ve čtyřech úrovních:

- IPMA Level A – certifikovaný ředitel projektu,
- IPMA Level B – certifikovaný projektový senior manažer,
- IPMA Level C – certifikovaný projektový manažer,
- IPMA Level D – certifikovaný projektový praktikant.

2.1.6 ISO 21 500

Na rozdíl od předchozích, se nejedná o certifikační standard a jeho obsahem je pouze soubor doporučení pro projektové řízení. Tematicky se jedná o standard, který je téměř shodný s PM BoK doplněný o informace týkající se kompetencí osob v řízení projektů (Doležal, 2016).

2.2 GDPR

Ochrana osobních údajů je v poslední době velmi mediálně propíraná, a to hlavně díky nařízení Evropské unie zvanému GDPR (General Data Protection Regulation). Právo na soukromí a osobní údaje patří mezi základní lidská práva a právní úprava pro zpracování osobních údajů se vyvíjí již od druhé poloviny dvacátého století. Ochrana osobních údajů tady tedy byla samozřejmě již před GDPR.

Dnešní doba vyniká výrazným rozvojem digitálních technologií a nárůstem zpracovávaných dat. Osobní data jsou zpracovávána stále více způsoby, na které mohla být aplikace stávající právní úpravy v mnoha případech dosti komplikovaná a v některých případech i nedostačující. Právě díky tomu se Evropská unie rozhodla modernizovat právní rámec pro ochranu osobních údajů, a tím zároveň sjednotit pravidla v jednotlivých členských zemích EU.

Dne 25. května 2018 vešlo v platnost Nařízení EU 2016/679, neboli Obecné nařízení o ochraně osobních údajů (General Data Protection Regulation, GDPR), které nahradilo většinu stávajících předpisů v této oblasti. Pomocí Nařízení je řešeno systematické nakládání s osobními údaji a je stanovena povinnost organizací doložit soulad svých činností s tímto nařízením, a to i zpětně. To souvisí také se zvýšením pokut za nesprávné zpracování dat (Nonnemann, 2018).

Dále jsou pomocí GDPR zaváděna konkrétnější a propracovanější pravidla pro zpracování osobních údajů a je kladen důraz na práva lidí dotčených zpracováváním. Mimo to určuje povinnosti správců a zpracovatelů, což zahrnuje zejména vedení záznamů o činnostech zpracování osobních údajů a následné posouzení vlivu zpracování údajů na jejich ochranu (DPIA) (Úřad pro ochranu osobních údajů, 2017).

Také je nutné zmínit, že Obecné nařízení o ochraně osobních údajů zavádí základní pravidla pro práci s osobními údaji, která nemusejí být dodržována pouze v případě, že dojde k zavedení zvláštní právní úpravy, která může upravit některé konkrétní aspekty zpracování osobních údajů v různých sektorech. Těmito sektory je myšlena například oblast zdravotnictví, školství, bankovnictví či kybernetické bezpečnosti. (Nonnemann, 2018).

Základním krokem pro práci s nařízením GDPR je definování, co je to osobní údaj. Osobní údaj je informace o fyzické osobě, pomocí níž lze tuto osobu jasně identifikovat. Jakmile je osoba jasně identifikována, každý další údaj vztahující se k této osobě, je možné již také považovat za osobní údaj (Nařízení EU 2016/679).

Dále je důležité definovat, co znamená zpracování osobních údajů. Osobní údaje jsou zpracovávány, jestliže jsou s nimi prováděny jakékoliv operace. Jedná se například o jejich shromažďování, čtení, kopírování, mazání, přepisování či vyhledávání.

Je potřeba také zmínit, že osoba jejíž údaje jsou zpracovávány, v Obecném nařízení označována jako subjekt údajů, má k těmto údajům určitá práva. Práva subjektů údajů jsou následující (Nařízení EU 2016/679):

- právo na informace o zpracování údajů,
- právo na přístup k údajům,
- právo na výmaz,
- právo na opravu,
- právo na omezení zpracování,
- právo na přenositelnost údajů,
- právo vznést námitku.

První zmíněné právo je na rozdíl od práv zbylých právo pasivní, což znamená, že aktivitu musí provést správce, aby subjektu poskytl informace (Úřad pro ochranu osobních údajů, 2017).

Zpracování osobních údajů může být prováděno na základě splnění následujících podmínek (Nařízení EU 2016/679).:

- zpracování je důležité pro plnění smlouvy,
- zpracování je důležité pro plnění právní povinnosti,
- zpracování je důležité pro ochranu životně důležitých zájmů,
- zpracování je důležité pro splnění veřejného zájmu nebo výkonu veřejné moci,
- zpracování je důležité pro oprávněné zájmy správce či třetí strany,
- subjekt údajů udělil souhlas se zpracováním.

Nejvíce nejasností ohledně podmínek pro zpracování osobních údajů bývá spojeno se souhlasem o zpracování těchto údajů. Mnoho lidí se domnívá, že nejlepší je souhlas požadovat vždy, to však není úplně pravda. Nezmar (2017) tvrdí, že souhlas je pouze jednou z možností a měl by být vyžadován pouze v případě, že neexistuje jiný zákonný důvod

pro zpracování osobních údajů. Typickým příkladem, kdy je požadováno udělení souhlasu, jsou marketingové a propagační účely. GDPR stanovuje, že souhlas musí být svobodný, konkrétní, jasně srozumitelný, informovaný a jednoznačný projev vůle subjektu. Splnit tyto podmínky je mnohdy velmi těžké. Jako příklad lze uvést situaci, kdy zaměstnavatel vyžaduje podepsání souhlasu po svém zaměstnanci a v tom případě může být podepsání souhlasu ovlivněno například strachem ze ztráty zaměstnání.

Existuje také zvláštní kategorie údajů, které jsou označeny jako citlivé. Jejich využíváním vzniká větší riziko poškození dotčených osob, a tak GDPR zavádí pro jejich zpracování přísnější podmínky. Do této skupiny patří rasa, náboženství, politický názor, informace o členství v odborech, zdravotní stav, sexuální orientace, genetické údaje a biometrické údaje. V Nařízení je uvedeno, kdy je zpracování těchto údajů možné, avšak pokud to není nutné, je dobré se těmto údajům vyhýbat (Úřad pro ochranu osobních údajů, 2017).

V Obecném nařízení je uvedeno 10 případů, ve který lze zpracovávat citlivé údaje. Jedná se o následující případy (Nařízení EU 2016/679):

- subjekt údajů udělil souhlas se zpracováním těchto údajů,
- zpracování je potřebné pro plnění právních povinností,
- zpracování je nezbytné na ochranu životně důležitých zájmů osob a subjekt údajů není schopný udělit souhlas,
- zpracování provádí nezisková organizace v rámci svých oprávněných činností, zpracování se týká jen jejich členů (i bývalých) nebo osob udržující s organizací pravidelné styky a osobní údaje nejsou bez souhlasu zpřístupněny mimo tuto organizaci,
- zpracování se týká zjevně zveřejněných osobních údajů,
- zpracování je potřebné pro soudní účely,
- zpracování je potřebné z důvodu veřejného zájmu,
- zpracování je potřebné z důvodu preventivního nebo pracovního lékařství, pro lékařskou diagnostiku, pro poskytnutí sociální a zdravotní péče či léčby a pro posouzení pracovní schopnosti,

- zpracování je důležité z důvodu veřejného zdraví, pro ochranu před vážnými přeshraničními zdravotními hrozbami,
- zpracování je pro účely archivace ve veřejném zájmu, pro vědecký nebo historický výzkum a pro statistické účely.

Za správce osobních údajů je považován jakýkoliv subjekt, který se rozhodne osobní údaje zpracovávat a má pro to řádný právní důvod. Jeho úkolem je také tyto údaje řádně a dostatečně zabezpečit.

Zpracovatel je subjekt provádějící zpracovávání údajů pro správce, odpovědnost za toto zpracovávání však stále nese správce. Správce a zpracovatel mezi sebou mají uzavřenou smlouvu o zpracování osobních údajů, která jasně vymezuje jejich vztah. Smlouva by měla obsahovat dobu, povahu, účel a předmět zpracování, dále typ údajů, způsob jejich zabezpečení a kategorii subjektu údajů. Dále určuje také práva a povinnosti správce i zpracovatele (Úřad pro ochranu osobních údajů, 2017).

Ve spojení s GDPR je často zmiňovaná role pověřence pro ochranu osobních údajů, anglicky Data Protection Officer (DPO). Jeho hlavními funkcemi je poskytování informací, kontrola, zda organizace zpracovává osobní údaje v souladu s nařízením, komunikace s Úřadem pro ochranu osobních údajů a školení pracovníků.

Významnou změnou, kterou přineslo GDPR, je zrušení oznamovací povinnosti správců. Tato povinnost byla do jisté míry nahrazena povinností správců vést Záznamy o činnostech zpracování, které slouží k prokázaní souladu s Obecným nařízením. Záznamy o činnostech zpracování nejsou povinny vést organizace, které mají méně než 250 zaměstnanců nebo je zpracovávají jen příležitostně. Avšak v případě velkého rizika poškození práv či svobod subjektů údajů tyto výjimky nelze považovat za platné (Nezmar, 2017).

V případě rizikových zpracování dat musí správce provést analýzu Posouzení vlivu na ochranu osobních údajů (Data Protection Impact Assessment, DPIA). Po této analýze by měla být přijata opatření pro zmírnění rizika. Pokud však riziko přetrvává, je nutné situaci konzultovat s Úřadem pro ochranu osobních údajů.

Součástí nařízení je také sankční část, která slouží jako preventivní a donucovací prostředek pro dodržování nařízení. Udělování pokut má na starosti dozorový úřad, který zajišťuje, aby tyto pokuty byly přiměřené a účinné pro každý jednotlivý případ. Při rozhodování o výši pokuty zohledňuje úřad například povahu, závažnost, úmyslnost

porušení, ale také kategorie osobních údajů dotčených porušením, předchozí možné porušování nařízení a mnohé další. V případě méně vážného porušení, se úřad může rozhodnout pouze pro udělení nápravných opatření. Obecně nařízení rozlišuje 2 hlavní kategorie pro udílení pokut podle závažnosti ohrožení chráněného zájmu stanoveného nařízením. V první kategorii lze udělit pokutu do 10 000 000 EUR nebo 2 % celkového ročního obratu podniku podle toho, která částka je vyšší. Do druhé kategorie patří nejzávažnější porušení podmínek nařízení, a proto za ně lze udělit pokutu do výše 20 000 000 EUR, či do 4 % celkového ročního obratu podniku, opět podle toho, která hodnota je vyšší (Žůrek, 2018).

Všechny osobní údaje, k jejichž zpracovávání v organizaci dochází, musejí být řádně zabezpečeny. Jestliže dojde k porušení zabezpečení, musí se zvážit, zda je potřeba incident ohlásit Úřadu pro ochranu osobních údajů či subjektu údajů. Porušení zabezpečení zahrnuje protiprávní zničení, ztrátu, změnu, neoprávněné poskytnutí a zpřístupnění osobních údajů. Ohlašovací povinnost nastává v případě ohrožení práv a svobod dotčených subjektů údajů (Nulíček, 2018).

Pokud taková situace nastane, musí se správce údajů ujistit, že opravdu došlo k vážnému porušení a bezodkladně tento incident ohlásit dozorovému úřadu. Ohlášení by mělo být provedeno do 72 hodin od vzniku incidentu a mělo by obsahovat popis porušení a kategorii zasažených údajů, kontakt na DPO, pravděpodobné následky porušení a popis přijatých opatření.

Pro zjištění nutnosti ohlašovat incident je dobré nejprve zjistit příčinu úniku dat, ověřit, zda incident stále probíhá (případně zamezit jeho dalšímu průběhu), zjistit rozsah škod a vypracovat analýzu dopadu (Úřad pro ochranu osobních údajů, 2017).

3 Metodická východiska řízení projektů

V následující kapitole jsou popsány základní a nejčastěji využívané metody projektového řízení. Teoretický popis a vymezení metod projektového řízení je nezbytné pro správné využití těchto metod v praktické části práce.

3.1 Projektový plán

Tvorba projektového plánu je proces definování, přípravy a koordinace podpůrných dokumentů, z nichž bude následně projektový plán sestaven. Hlavním přínosem projektového plánu je vytvoření centrálního dokumentu, ve kterém budou popsány a definovány základy celkové projektové práce.

Projektový plán udává, jak bude projekt řízen, vykonáván, monitorován, kontrolován a uzavřen. Jeho obsah se obvykle různí a závisí na typu, oblasti a velikosti projektu (Project Management Institute, 2013).

Následující kapitoly se zabývají dokumenty a technikami, které jsou často součástí projektového plánu.

3.2 Studie proveditelnosti

Jedním z nejdůležitějších dokumentů zpracovávaných před zahájením projektu je studie proveditelnosti. Účelem studie proveditelnosti je posouzení realizovatelnosti projektu a zhodnocení jednotlivých alternativ realizace. Jedná se o rozhodující dokument, na jehož základě je projekt realizován a vede k rozhodnutí o investici. Studie proveditelnosti bývá velmi rozsáhlá a většinou jí zpracovává větší tým odborníků (Sieber, 2004).

Ministerstvo vnitra České republiky (2019) uvádí patnáct bodů/kapitol, které by měla studie proveditelnosti obsahovat. První kapitola by měla obsahovat název projektu, jeho zpracovatele a zadavatele, včetně kontaktních údajů na ně a identifikaci dokumentu, tzn. že v ní musí být uvedeno, že se jedná o studii proveditelnosti. Druhým bodem studie proveditelnosti je popis výchozího stavu, uvedení důvodu realizace projektu a analýza potřebnosti, případně přínosu projektu. Následující kapitola se má zaobírat hlubším popisem projektu, jeho jednotlivých částí a aktivit. Zmíněn zde bývá také investor projektu, nezbytná legislativa a specifikace projektu. Čtvrtá kapitola má obsahovat informace o projektovém týmu a způsobu řízení projektu. V páté kapitole jsou obvykle řešeny technické

a technologické aspekty projektu, výhody a nevýhody jednotlivých technologických řešení a věci s tímto spjaté. Následně jsou řešena kritéria výběru řešení projektu po organizační, technologické a procesní stránce, společně se stručným popisem nejvhodnější varianty. Sedmá kapitola je většinou zaměřena na zajištění projektu, což obsahuje vymezení výše nákladů a majetku projektu. V osmé kapitole bývá popsán harmonogram projektu, často také znázorňovaný pomocí Ganttova diagramu. Devátá kapitola by měla obsahovat finanční a ekonomické analýzy. V dalším bodě je obvykle zhodnocena efektivita projektu pomocí ukazatelů finančních toků. Velmi důležitá je jedenáctá kapitola, jejíž součástí je analýza a řízení rizik. Dále je obvykle řešen vliv projektu na životní prostředí. Poslední tři kapitoly by měly obsahovat zhodnocení projektu na základě provedených analýz, včetně shrnutí jejich hlavních závěrů, doporučení a upozornění pro případnou realizaci projektu a použité zdroje.

Je samozřejmé, že co se týká robustnosti a podrobnosti zpracování studie proveditelnosti, záleží hlavně na typu a významu projektu. Existují projekty, u kterých lze některé kapitoly vynechat, a naopak na jiné musí být kladen zvláštní důraz.

3.3 Work Breakdown Structure (WBS)

WBS (Work Breakdown Structure) neboli hierarchická struktura prací je analytická metoda projektového řízení, založená na rozkladu cíle projektu na menší dodávky a subdodávky. Nejnižším stupněm rozkladu jsou takzvané pracovní balíky. Přínosem této metody je lepší představa o tom, co musí být dodáno (Project Management Institute, 2013).

Jedná se o jeden z nejpodstatnějších dokumentů řízení projektu obsahující podklady pro řízení časového plánu, nákladů, zdrojů a změn v projektu. V rámci WBS je také definován celkový rozsah projektu.

Důležitou součástí každé WBS jsou takzvané milníky. Milníky jsou velmi podobné běžným aktivitám v projektu, avšak jejich doba trvání je nulová. Představují určitý významný okamžik v čase a často se může jednat například o předávání části výstupu zákazníkovi.

Pomocí WBS je definováno, co má být uděláno, ale není zde již popsáno, jak nebo kdy to má být uděláno. Metoda bývá často zobrazována v podobě úkolově orientovaného stromu, jehož kořenem je právě cíl projektu. Nejedná se však o jediný možný způsob zobrazení WBS, další možností je například tabulkový formát, který využívá Microsoft Project.

Lišit se však nemusí jen formát zobrazení WBS, ale také to, jaký je zvolen přístup dekompozice. WBS může být uspořádáno podle projektových fází, produktů projektu nebo skupin procesů. Nejnižší prvek v hierarchické struktuře bývá často nazýván Pracovní balík, jedná se o úkol, který už nelze dále dělit a může mít přiřazen odhad doby trvání (Schwalbe, 2011).

Schwalbe (2011) uvádí, že jedním z možných přístupů k vytvoření WBS je aplikace myšlenkových map. Tento přístup nemá pevně stanovenou strukturu, je spíše vizuální a tím rozvíjí kreativitu a uvolňuje možné napětí v projektovém týmu. Po dokončení myšlenkové mapy jí lze samozřejmě převést do klasičtější formy WBS v podobě tabulky či diagramu.

K samotné WBS je vhodné přiložit také její slovník. Jedná se o dokument obsahující detailní informace o jednotlivých položkách WBS. Informace obsažené ve slovníku se budou lišit v závislosti na typu projektu, avšak často v něm můžeme najít zdroje, čas zpracování, náklady a odpovědnou osobu za zpracování dané položky.

WBS společně se svým slovníkem a výkazem o rozsahu projektu (obsahuje popis rozsahu projektu, hlavní výsledky a cíle, předpoklady a omezení projektu) tvoří směrný plán projektu, který je nedílnou součástí projektového plánu (Project Management Institute, 2013).

3.4 Critical Path Method (CPM)

Metoda kritické cesty (Critical Path Method) je metodou síťové analýzy, využívanou pro odhadnutí celkové doby trvání projektu a určení míry flexibility (časových rezerv) této doby. Pomocí CPM jsou vypočítávány nejdříve možné začátky, nejdříve možné konce, nejpozději možné začátky a nejpozději možné konce všech aktivit v rámci projektu. Kritická cesta projektu je posloupnost aktivit reprezentujících nejdelší cestu v projektu s nejkratší možnou dobou trvání, za kterou lze projekt dokončit. Tato cesta nemá žádné časové rezervy a její aktivity jsou nazývány kritické aktivity.

Časová flexibilita (či rezerva) je dána pomocí času, o který může být naplánována aktivita opožděná či prodloužená, aniž by došlo k opoždění dokončení projektu (Project Management Institute, 2013).

Datum dokončení projektu je určováno na základě kritické cesty, která je cestou nejdelší. V projektu však obvykle existují i jiné cesty, což je způsobeno probíháním několika

aktivit současně. Právě aktivity na těchto vedlejších cestách mohou obsahovat časové rezervy (Schwalbe, 2011).

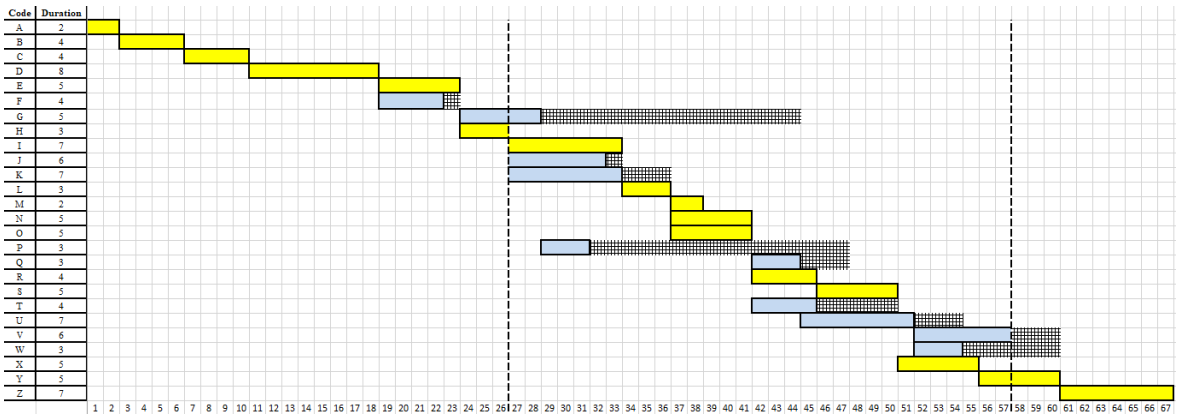
Pro výpočet kritické cesty je nutné, s využitím aktivit naplánovaných ve WBS, nejprve vytvořit síťový graf. Každé aktivitě musí být přiřazena její odhadnutá doba trvání, a také musí být jasně stanoveno jejich následovnictví. Odhadnuté doby trvání se následně na jednotlivých cestách sečtou a cesta s nejdelší dobou trvání je označována jako kritická (Fiala, 2004).

V průběhu projektu se jednotlivé aktivity a jejich doby trvání mohou měnit, a tak je nutné udržovat síťový graf neustále aktuální (Schwalbe, 2011).

3.5 Ganttův diagram

Ganttovy diagramy jsou sloupcové grafy využívané v projektovém řízení ke grafickému zobrazení časového harmonogramu aktivit v projektu. Jednotlivé aktivity jsou zachyceny na svislé ose grafu, zatímco na vodorovné ose je vyznačen čas. Každá aktivita v projektu je zobrazena jako vodorovný sloupec umístěný do grafu v závislosti na datu svého zahájení a dokončení. Výhodou těchto grafů je, že jsou lehce čitelné a srozumitelné, a tak je velmi jednoduché je prezentovat například zákazníkovi či vedení firmy (Project Management Institute, 2013).

Jak už bylo zmíněno, diagram zachycuje všechny aktivity projektu uvedené v rámci WBS, a to včetně milníků projektu. Ty mohou zobrazovat důležité události nebo dílčí cíle projektu a měly by být SMART, tedy specifické, měřitelné, přiřaditelné, realistické a časově ohraničené (Svozilová, 2016).



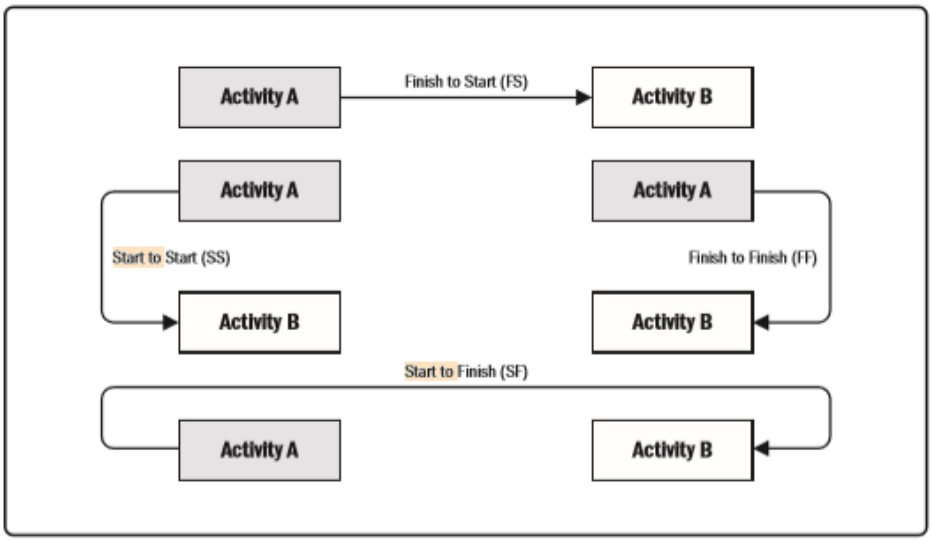
Obrázek 3.1 Ganttův diagram (zdroj: vlastní zpracování)

Na obrázku číslo 3.1 je možné vidět příklad zpracování Ganttova diagramu pomocí tabulkového procesoru Microsoft Excel. Kritická cesta je vyznačena žlutě a nekritické aktivity jsou vyznačeny modře. U nekritických aktivit lze také pozorovat jejich časové rezervy vyznačené mřížkou.

Ganttův diagram lze samozřejmě zpracovat pouze pomocí tužky a papíru, avšak v dnešní době lze najít mnoho online nástrojů, které pomáhají práci velmi urychlit. Dobrým a často využívaným nástrojem, nejen pro tvorbu těchto diagramů, je softwarový nástroj Microsoft Project. Tento projektový nástroj bývá využíván již při tvorbě WBS, kde následně každé aktivitě umožňuje přiřadit časovou náročnost, potřebné zdroje a vazby na další činnosti projektu. Na základě takto vytvořené WBS poté automaticky program vygeneruje Ganttův diagram.

Důležitou součástí při plánování projektu a tvorbě Ganttova diagramu jsou již zmíněné vazby činností. V projektu lze využít čtyři typy vazeb (Project Management Institute, 2013):

- Finish-to-Start – činnost B nemůže začít, dokud není ukončena činnost A,
- Start-to-Start – činnost B nemůže začít, dokud nezačne činnost A,
- Finish-to-Finish – činnost B nemůže skončit, dokud neskončí činnost A,
- Start-to-Finish – činnost B nemůže být ukončena, dokud nezačne činnost A.



Obrázek 3.2 Typy vazeb činností v projektu (zdroj: Project Management Institute, 2013)

3.6 Řízení rizik

Velmi důležitou oblastí projektového managementu je oblast řízení rizik. Řízení rizik zahrnuje další podoblasti, jakými jsou identifikace rizik, analýza rizik, plánování odpovědí na rizika a kontrola rizik.

Riziko projektu lze definovat jako nejistou událost, která když nastane, tak má negativní či pozitivní dopad na projekt (jeho rozsah, časový plán, náklady nebo kvalitu). Pozitivní a negativní rizika bývají označovány jako příležitosti a hrozby. Organizace a zainteresované osoby jsou mnohdy ochotni riziko v různé míře akceptovat. Vše záleží na velikosti rizika, velikosti odměny a postoji jednotlivých osob k rizikům (Projekt Management Institute, 2013).

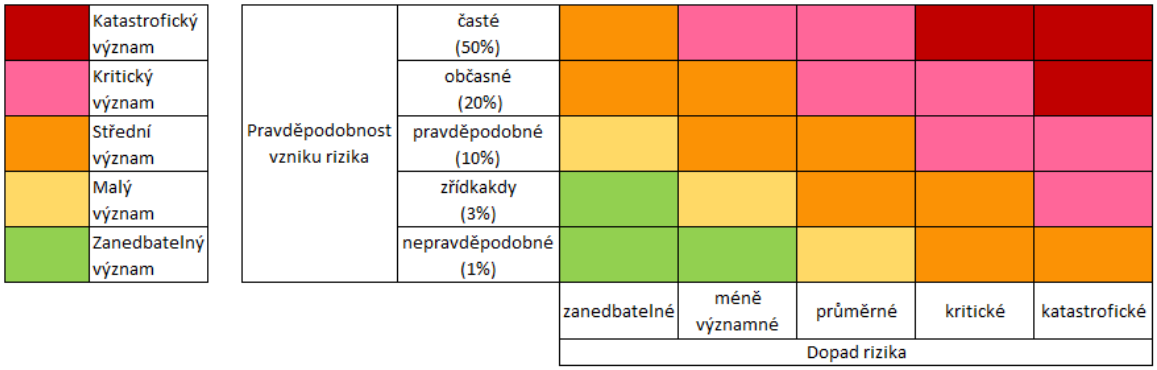
Součástí projektového plánu je vždy také plán řízení rizik. Tento plán by měl vždy obsahovat informace o vybrané metodě řízení rizik, rozdělení odpovědností, náklady spojené s riziky, časový plán pro řízení rizik, kategorie možných rizik a stanovení pravděpodobnosti a dopadu pro různá rizika.

Jako základ pro řízení rizik v organizacích existuje mnoho metod, nástrojů a technik určených hlavně pro identifikaci a analýzu rizik.

Prvním důležitým krokem řízení rizik je samotná jejich identifikace. K tomuto účelu je často využívaná metoda s názvem brainstorming a další tvůrčí nástroje a techniky, jako jsou například již zmiňované myšlenkové mapy nebo takzvaný diagram příčin a následků neboli Ishikawův diagram. Důležité také bývá vypracování SWOT analýzy.

Často bývá výhodné vycházet z předchozích projektů a rizik, které byly již v minulosti analyzovány. Na procesu plánování a identifikaci rizik by se měl podílet nejen celý projektový tým, ale také další stakeholdeři, ať mohou být analyzována rizika z rozdílných úhlů pohledu.

Při identifikaci rizika je nezbytné provést jeho podrobný popis, včetně určení příčiny vzniku (hrozby), pravděpodobnosti vzniku, dopadu a významu rizika. Nástrojem pro určení významu rizik je matice pravděpodobnosti a dopadu. Význam rizik bývá dán součinem pravděpodobnosti a rizika (Řeháček, 2013). Příklad takovéto matice lze vidět na obrázku 3.3.



Obrázek 3.3 Matice pravděpodobnosti a dopadu rizik (zdroj: vlastní zpracování)

Pro další hodnocení a řízení rizik je možné využít Paretova pravidla, které říká, že relativně malé procento rizik (těch nejzávažnějších), tedy asi 20 %, způsobuje nejvíce problémů v projektu, a to okolo 80 %. Z toho vyplývá, že se vyplatí řešit ta nejzávažnější rizika a nevynakládat prostředky na řešení těch málo závažných (Doležal, 2013).

Mezi metody zabývající se celkovým postupem pro řízení rizik v projektu patří metoda FMEA. Failure Mode and Effect Analysis (FMEA) neboli Analýza možnosti vzniku vad a jejich následku je metoda využívaná hlavně u projektů z oblasti výrobního průmyslu. Tato metoda vyžaduje zapojení celého projektového týmu a lidí z různých oblastí výroby produktu.

Další hojně využívanou metodou řízení rizik je metoda CRAMM (CCTA Risk Analysis and Management Method). Jedná se o metodu zabývající se hlavně bezpečnostními riziky informačního charakteru. U projektů spojených s potravinami bývají rizika řízena pomocí metody Hazard Analysis and Critical Control Points (HACCP).

Výše zmíněné metody se zabývají hlavně řízením rizik produktů z nejrůznějších oblastí. Takovýchto metod existuje samozřejmě mnohem více, a to nejen z oblasti řízení rizik produktů, ale také z oblasti řízení rizik managementu projektu, jejich obsah však není předmětem této diplomové práce (Doležal, 2013).

Dobré je také zmínit směrnici ISO 31000, která je důležitým standardem pro řízení rizik v organizacích. Jedná se o standard poskytující návody, jak snadno a spolehlivě řídit rizika v organizacích jakéhokoliv typu a zaměření.

V souvislosti se zpracováním osobních údajů musí také nutně docházet k řízení rizik. K tomuto účelu se v této oblasti využívá již výše zmíněná analýza DPIA (Data Protection Impact Assesment) neboli Posouzení vlivu na ochranu osobních údajů. Posouzením vlivu

na ochranu osobních údajů se zabývá článek 35 Obecného nařízení, kde je obecně vymezeno, kdy je nutné tuto analýzu provádět. Podrobnější druhy operací podléhající Posouzení vlivu na ochranu osobních údajů vydává podle Nařízení dozorový úřad čili Úřad pro ochranu osobních údajů. Podrobněji je analýza DPIA popsána ve 4. kapitole této práce.

4 Analýza současného stavu a požadavků GDPR

Tato kapitola je zaměřena na prostředí, v němž je diplomová práce zpracována a zároveň na obecné vymezení jednotlivých kroků, jejichž provedení je důležité pro správnou implementaci požadavků GDPR.

4.1 Gymnázium BESKYDY MOUNTAIN ACADEMY, s.r.o.

Gymnázium BESKYDY MOUNTAIN ACADEMY, s.r.o. (dále jen BMA) je soukromá škola nacházející se ve Frýdlantu nad Ostravicí, jejímž zřizovatelem je spolek THE BESKYDY MOUNTAIN ACADEMY. Jedná se o čtyřleté gymnázium specializující se na výuku angličtiny. Škola, která vznikla v roce 2003, měla být původně dvojjazyčná, avšak kvůli těžkostem s realizací původní představy bylo založeno gymnázium zaměřené na výuku jazyků a prohlubování křesťanských hodnot. Jelikož se jedná o soukromou školu, která je státem financována jen z části, studenti jsou povinni platit za studium školné.

Jelikož je nařízení GDPR platné již téměř rok, dá se předpokládat, že všechny požadavky vyplývající z GDPR jsou již ve škole aplikovány. V současnosti je však plánovaná rekonstrukce, jejíž součástí má být také zvýšení bezpečnosti ve škole. Z důvodů zvýšení bezpečnosti již škola zavedla přístupový systém založený na čipových kartách a plánuje jej ještě doplnit kamerovým systémem. Za tímto účelem musí být u nově vzniklých procesů zpracování osobních údajů zajištěna aplikace požadavků vyplývajících z GDPR. Zároveň bude zmapována současná situace aplikování GDPR v organizaci a budou navrženy případné změny.

4.2 Analýza požadavků GDPR

Výchozím krokem pro práci v oblasti zpracovávání osobních údajů a GDPR je důkladné prostudování Obecného nařízení o ochraně osobních údajů. Na základě Obecného nařízení lze vymezit několik kroků, kterými je nutné se při zavádění GDPR v organizaci řídit. Nápomocný může být také dokument vydaný MŠMT (Ministerstvo školství, mládeže a tělovýchovy) Metodická pomůcka k aplikaci GDPR, v němž jsou zachyceny náležitosti, které je nutné v souvislosti s GDPR zajistit. Ze všeho nejdříve by měly být identifikovány a analyzovány veškeré osobní údaje a k nim se vztahující procesy, ke kterým v dané organizaci dochází. Dalším krokem je zhodnocení požadavků na jmenování DPO (Data Protection Officer) a výběr vhodného kandidáta. Následně je obecně doporučováno

provedení analýzy GAP, která má za úkol zjistit, zda a jak moc je organizace v souladu s požadavky GDPR. V případě zjištění odchylek v oblasti zajištění osobních údajů od požadavků GDPR musí být provedena nápravná opatření a aplikovány požadavky Obecného nařízení. Pokud budou odhalena riziková zpracování osobních údajů, musí dojít k vypracování analýzy DPIA (Posouzení vlivu na ochranu osobních údajů) a následné aplikaci navržených úprav zpracování. Po provedení všech základních kroků nezbytných pro správnou implementaci požadavků GDPR by měla být veškerá práce revidována a dále pravidelně kontrolována.

4.2.1 Analýza procesů zpracování dat

Prvním krokem, který by měl být proveden, je analyzování procesů, při nichž dochází ke zpracovávání osobních údajů, ale také dat samotných. Provedení analýzy je nutné ke správnému vypracování karty záznamů o činnostech zpracování, která je výstupem této analýzy.

Vedení záznamů o činnostech zpracování je povinné na základě článku 30 Obecného nařízení. Za vedení těchto záznamů je odpovědný správce. Jeho kontaktní údaje, kontaktní údaje jeho zástupce, ale také pověřence pro ochranu osobních údajů, pokud jej daná organizace má, musí být součástí karty záznamů o činnostech zpracování.

Karta záznamů musí obsahovat hlavně popisy všech možných zpracování osobních údajů, ke kterým v dané organizaci dochází. Ke každému účelu zpracování je přiřazen popis jednotlivých kategorií subjektu údajů, kterých se dané zpracování týká. V oblasti školství budou mezi obvyklými subjekty údajů vždy hlavně zaměstnanci školy, žáci/studenti, rodiče a zákonní zástupci nezletilých. Mezi subjekty údajů mohou často patřit také osobní údaje dodavatelů a dalších třetích stran. Samozřejmě musí být popsány kategorie osobních údajů a konkrétní osobní údaje, které se daného zpracování týkají.

Další náležitosti, které by měly být uvedeny u každého záznamu o zpracování jsou právní tituly na jejichž základě mohou být data zpracovávána, údaj o nutnosti zpracování, zdroje, ze kterých jsou osobní údaje získávány, předpokládaná doba, po kterou budou data zpracována, místo fyzického uložení dat, způsob případné likvidace dat, popis osob, které mohou s daty manipulovat (včetně určení způsobu manipulace), záznamy o předávání dat mimo organizaci, informace o zpracovateli, odkaz na interní předpis na jehož základě jsou

data zpracovávána, popis bezpečnostních opatření, včetně způsobu zálohování a popis případných odchylek od legislativy, které je nutno odstranit.

Zde je vypsáno několik příkladů procesů, při nichž dochází ke zpracování osobních údajů ve školách:

- Zpracování OÚ zaměstnanců – podklady pro výběrová řízení, vedení databáze uchazečů, personální a mzdová evidence, evidence školení, poskytování benefitních programů, zajištění externího vzdělávání atd.
- Zpracování OÚ studentů – podklady pro přijetí, vedení školní matriky, vedení docházky, kniha úrazů, pořádání vzdělávacích kurzů, účast na soutěžích, propagace školy atd.
- Zpracování OÚ rodičů – evidence kontaktů pro naléhavé případy, sdělování údajů o prospěchu studenta, placení výdajů spojených se vzděláním atd.

Výše uvedené příklady, jsou pouze vzorové procesy, ke kterým ve školách velmi často dochází. Některé z nich, jako například vedení školní matriky, vyžaduje školský zákon, a tak je musí provádět každá škola. V závislosti na konkrétní škole pak mohou být další procesy a subjekty údajů doplněny či odebrány.

4.2.2 Jmenování pověřence pro ochranu osobních údajů

Jak již bylo uvedeno v předchozích kapitolách, jedna z povinností, kterou přineslo Obecné nařízení GDPR, je jmenování pověřence pro ochranu osobních údajů. Je nutné zdůraznit, že povinnost jmenování pověřence neplatí pro každou organizaci. V Obecném nařízení jsou uvedeny tři případy, kdy musí mít dané organizace vždy jmenovaného pověřence. Za prvé musí mít jmenovaného pověřence všechny veřejné subjekty a orgány veřejné moci, mimo soudy. Za druhé musí mít pověřence každá instituce, jejíž hlavní činností je zpracovávání osobních údajů a je důležité pravidelné kontrolování aktuálnosti údajů. Posledním případem, kdy musí mít podle GDPR instituce jmenovaného pověřence, je, když součástí její hlavní činnosti je objemné zpracovávání citlivých údajů či údajů o trestných činech osob.

Pověřencem může být jak zaměstnanec instituce, tak i externí pracovník. Vždy by se mělo jednat o osobu, která má odborné znalosti v oblasti ochrany osobních údajů, včetně právních předpisů a nařízení. Jedná se o kontaktní osobu organizace, jestliže se chce někdo

informovat o zpracování svých osobních údajů. V případě, že je pověřenec interním zaměstnancem, je nutné dbát na to, aby byla dodržena jeho nezávislost na procesech, které má jako pověřenec hodnotit.

Mezi hlavní úkoly pověřence, rovněž uvedené v Obecném nařízení, patří pomoc a poskytnutí rad a informací správcům a zpracovatelům, tak aby jejich znalosti byly aktuální a přesné, kontrola, že je instituce v souladu s obecným nařízením, a to včetně zabezpečení, hodnocení rizik a evidence osobních údajů, pomoc při zpracování DPIA a navržení metodiky analýzy rizikového zpracování, kooperace s dozorovým úřadem ve všech případech týkajících se zpracování osobních údajů a již zmíněné plnění funkce kontaktní osoby v souvislosti s GDPR. Mezi jeho povinnosti nepatří tvorba jakýchkoliv dokumentů spojených se správnou implementací GDPR, ale spíše poskytování konzultací a rad lidem, kteří tyto dokumenty tvoří.

Pro účely této diplomové práce je zásadní definovat, v jakých případech musí být jmenován pověřenec pro ochranu osobních údajů ve školách. Ministerstvo vnitra ve spolupráci s Úřadem pro ochranu osobních údajů zpracovalo metodické doporučení zabývající se právě tématikou pověřence pro ochranu osobních údajů. V tomto dokumentu je mimo jiné uvedeno, že každá školská právnická osoba může rozhodovat o právech a povinnostech osob (proto jí lze považovat za orgán veřejné moci), a tedy musí mít pověřence pro ochranu osobních údajů. Jinými slovy, pověřence musí mít každá škola, ať už je veřejná či soukromá.

4.2.3 GAP analýza

GAP analýza, často také nazývána jako analýza tržních mezer či diferenční analýza, je původní analýzou využívanou v oblasti marketingu a strategického řízení, avšak může být zpracována pro jakoukoliv jinou oblast. Tato analýza je používána ke zjištění rozdílů mezi aktuálním stavem a stavem požadovaným. V souvislosti s GDPR jsou pomocí GAP analýzy porovnávány požadavky nařízení se skutečným stavem ochrany osobních údajů v organizaci. Jejím výstupem je popis zjištěných rozdílů mezi stavem požadovaným a skutečností a návrh potřebných opatření pro dosažení požadovaného stavu.

Při provádění této analýzy pro oblast GDPR je důležité soustředit se hlavně na:

- identifikaci procesů a osobních údajů v nich zpracovávaných,
- dokumentaci, která je v rámci GDPR požadovaná a na správnost jejího zpracování,
- povinnost jmenování DPO,
- vhodnost zabezpečení osobních údajů a procesů jejich zpracovávání,
- vědomosti a vyškolenost zaměstnanců v oblasti osobních údajů.

Po provedení analýzy a zjištění případných rozdílů, je nutné provést všechna navržená opatření, aby byla organizace v souladu s nařízením GDPR.

4.2.4 DPIA analýza

Jestliže v některém z předchozích kroků bylo identifikováno zpracovávání osobních údajů, které by mohlo být považováno za rizikové, musí být provedeno posouzení vlivu tohoto zpracování na ochranu osobních údajů. Obecně platí, že tato analýza by měla být provedena ještě před zahájením rizikového zpracování osobních údajů. Na základě Obecného nařízení musí být zpracováno posouzení vlivu na ochranu osobních údajů vždy, pokud se jedná o monitorování veřejných prostorů, objemné zpracování citlivých údajů nebo automatizované zpracování údajů a profilování. Zpracování konkrétnějšího listu případu, kdy je anebo není nutné provádět analýzu, má za úkol stanovit dozorový úřad.

Úřad pro ochranu osobních údajů vydal třináctistránkový dokument zabývající se právě povinnostmi správců provádět DPIA (Data Protection Impact Assessment). V tomto dokumentu dozorový orgán stanovil základní kritéria, podle nichž má správce za úkol posoudit rizikovost procesů. Podle těchto kritérií následně vytvořil úřad 10 typů zpracování, na které se obecně povinnost vypracování DPIA vztahuje. U každého typu zpracování jsou navíc stanoveny 3 skupiny hodnot, jichž může konkrétní zpracování nabývat. Tyto skupiny určují významnost rizika a rozdělují jej na kritické hodnoty, významné hodnoty a nízké hodnoty. Úkolem správce je správně charakterizovat a zařadit posuzované zpracovávání osobních údajů, a podle množství kritických a významných hodnot rozhodnout o nutnosti zpracování DPIA.

V případě, že si správce není jistý, zda musí DPIA zpracovávat, je doporučeno analýzu raději vypracovat. V případě zjištění vysoké rizikovosti zpracování je nutné přijmout opatření pro zmírnění rizik, případně konzultovat toto zpracování s dozorovým úřadem.

Jak by mělo posouzení vlivu na ochranu osobních údajů vypadat, není nikde striktně uvedeno, avšak podle Obecného nařízení musí DPIA obsahovat alespoň (Nařízení EU 2016/679):

- popis plánovaných zpracování, účel zpracování a případně oprávněné zájmy správce,
- posouzení nezbytnosti a přiměřenosti zpracování v závislosti na jeho účelu,
- posouzení rizik pro práva a svobodu subjektů,
- popis plánovaných bezpečnostních a jiných opatření, aby byl zajištěn prokazatelný soulad s GDPR.

Konečná podoba zpracování DPIA tedy záleží na člověku, který jí bude zpracovávat. Vhodným přístupem k vypracování analýzy je popis a zhodnocení zpracovaní ve čtyřech oblastech – oprávněnost, zabezpečení, dopad a rozsah. Pro vyhodnocení rizikovosti je dobré každé oblasti přiřadit váhu a porovnat váhy oprávněnosti a zabezpečení procesu zpracování s váhami jeho dopadu a rozsahu. Jestliže je zpracování vysoce rizikové, budou váhy dopadu a rozsahu nabývat větších hodnot, a tedy je nutno přijmout nápravná opatření, případně situaci konzultovat s dozorovým úřadem.

Jelikož škola BMA plánuje v rámci rekonstrukce zavedení kamerového systému, bude provedení analýzy DPIA nezbytné.

4.2.5 Interní postupy a směrnice

Pro jednotný přístup všech zaměstnanců k osobním údajům zpracovávaných v rámci organizace je důležité důkladné vypracování a pravidelná kontrola interních směrnic. Všechny interní směrnice a dokumenty obsahující pracovní postupy související se zpracováním osobních údajů v organizaci by měly být neustále aktualizovány tak, aby splňovaly požadavky GDPR.

Součástí interní dokumentace by mělo být také vedení evidence všech získaných souhlasů, evidence požadavků na naplnění práv subjektu údajů a jejich včasného zpracování, evidence školení zaměstnanců, evidence porušení zabezpečení a dokumentace organizační

struktury, včetně odpovědností. Všechny tyto dokumenty mohou pomoci ve snadnější komunikaci uvnitř organizace, ale také v případě kontroly dozorovým úřadem.

Při implementaci GDPR v organizaci, je velmi dobré vést deník implementace, v němž budou popsány jednotlivé kroky a rozhodnutí, společně s odůvodněním těchto rozhodnutí. Tento deník implementace se může opět velmi hodit při kontrole dozorového úřadu.

5 Návrh procesu implementace GDPR ve školství

Obsahem této kapitoly je implementace požadavků nařízení GDPR ve škole BMA. V praxi často nastávají při zavádění GDPR v institucích problémy týkající se stanovení časového rámce, nákladů, ale i samotné organizace implementace požadavků. Tím mnohdy dochází k vytváření chaosu a obecných obav z GDPR. Za účelem zmírnění těchto problémů jsou v této práci využívány postupy a metody projektového řízení. Zároveň je důležité postupovat podle obecných kroků implementace, vymezených v předchozí kapitole.

5.1 Plán projektu GDPR

Jakmile se organizace rozhodne pro implementaci požadavků GDPR či pro provádění změn s GDPR souvisejících, je nejdůležitějším krokem veškerou práci naplánovat a správně zorganizovat. Pro tento účel je dobré vytvořit plán projektu obsahující alespoň hierarchickou strukturu prací a základní studii proveditelnosti.

5.1.1 Studie proveditelnosti pro zavedení kamerového systému

Jak již bylo zmíněno v teoretické části práce, studie proveditelnosti je jedním z nejdůležitějších dokumentů při tvorbě projektů, jelikož udává základní představu, proč a jak je nutné projekt vytvořit, a také mnohdy odhaluje, zda je to vůbec možné. Z toho důvodu je tvorba této studie také prvním krokem praktické části práce.

Úvod

Následující text zachycuje základní návrh studie proveditelnosti pro projekt s názvem Implementace požadavků GDPR.

Zadavatelem projektu je Gymnázium BESKYDY MOUNTAIN ACADEMY, s.r.o.

Zpracovatelem projektu je Anna Vaňková ve spolupráci s panem Pavlem Říhou.

Výchozí stav a důvod realizace projektu

Gymnázium BMA je soukromá škola, která již delší dobu plánuje rekonstrukci budovy školy, jejíž součástí by mělo být navýšení počtu učeben. Tyto učebny se budou nacházet v nově vystavěném 3. nadzemním podlaží. Společně s nově vystavěným podlažím je naplánovaná výstavba terasy v prostoru střechy. Po dokončení rekonstrukce požaduje

vedení organizace lepší zabezpečení prostorů školy. K rozsáhlejšímu zabezpečení budovy by mělo dojít pomocí zavedení kamerového systému.

Se zavedením kamerového systému v prostorách školy vznikají nové povinnosti v souvislosti s Obecným nařízením GDPR. Z toho důvodu je nutné vypracovat projekt, jehož cílem je zavedení kamerového systému vyhovující požadavkům GDPR.

Budova školy má v současné době před rekonstrukcí 2 nadzemní patra a dovnitř se lze dostat ze 2 vchodů. Hlavní vchod se nachází na straně hlavní ulice a je využíván žáky, zaměstnanci, rodiči a veřejností, která využívá služeb jídelny. Druhý vchod, kterým se lze do školy dostat, je na levé straně budovy a vede přímo do školní jídelny. Tento vchod využívají zaměstnanci jídelny a také slouží jako vchod pro zásobování. Je důležité zdůraznit, že jídelna není součástí školy a je provozovaná samostatně.

Dveře do hlavního vchodu budovy jsou prosklené a v době provozu školy jsou trvale otevřeny. Za těmito dveřmi se nachází zádveří, oddělené od zbytku školy dalšími uzamykatelnými dveřmi, které jsou ovládány elektrickým zámkem. Elektrický zámek dveří je napojen na přístupový systém budovy spojený se čtečkou karet umístěnou v zádveří. Studenti a zaměstnanci školy mají přístupové karty, které po přiložení ke čtečce dveře otevřou. Další návštěvy, kterými mohou být například rodiče, musí pomocí dveřního komunikátoru zazvonit na sekretariát, odkud jim jsou dveře vzdáleně otevřeny pomocí telefonní linky. V zádveří se nacházejí ještě další dveře, vedoucí do školní jídelny. Tyto dveře jsou využívány také veřejností a nejsou nijak speciálně zabezpečeny.

V přízemním patře školy se nacházejí šatny pro studenty, multimediální učebna a již zmiňovaná jídelna. Do jídelny mají studenti a učitelé přístup z vnitřního prostoru školy. U tohoto vstupu není zavedena žádná kontrola, a je tedy možné, aby kdokoliv, kdo projde volným vstupem ze zádveří budovy do jídelny, dále volně pokračoval tímto vstupem do vnitřních prostor školy. Tímto způsobem může docházet k neoprávněným vstupům do prostor školy.

Multimediální učebna, která se, jak již bylo zmíněno, nachází rovněž v přízemním patře budovy, je přístupná pouze z vnitřních prostor školy. Jelikož již byla tato místnost v minulosti vykradena, jsou její okna vybavena ochrannými mřížemi.

Celé přízemí bude zabezpečeno pomocí tří kamer. První kamera bude umístěna v zádveří a bude sloužit k identifikaci osob vstupujících do budovy. Další kamera bude

monitorovat prostory šaten a poslední bude pro monitorování vstupu do multimediální učebny, vstupu do jídelny pro studenty a zaměstnance a prostoru schodiště.

Zbylá dvě nadzemní patra a třetí nově plánované patro mají stejný půdorys jako přízemí budovy. Po vystoupení ze schodiště do patra se po pravé straně nachází vstupy do jednotlivých učeben, naproti schodiště jsou kanceláře a po levé straně se nacházejí toalety. Ve všech třech podlažích bude naplánováno umístění kamer stejným způsobem. Jedna z kamer bude sledovat prostor schodiště a vstup do jednotlivých učeben, druhá kamera bude umístěna na stěně nad okny, tak aby sledovala prostor chodby a vstupy do kanceláří. Monitorování vstupů na toalety je potřeba se vyhnout.

Jelikož je zavedení kamerového systému velkým zásahem do soukromí osob, má velký vliv na osobní údaje subjektů a za porušení Obecného nařízení mohou být uděleny velké pokuty, je nutné se v tomto případě detailně problematikou požadavků GDPR zabývat. Toho lze nejlépe dosáhnout pomocí tvorby projektu, v němž budou zachyceny všechny potřebné kroky s tím související.

Přínosem projektu bude lepší zabezpečení osob a majetku ve škole, přičemž budou dodržovány veškeré zásady GDPR.

Popis projektu

Projekt je realizován na základě zadání požadavku soukromého gymnázia ve Frýdlantu nad Ostravicí, o zvýšení bezpečnosti v souladu s požadavky GDPR.

V rámci projektu se není potřeba zaobírat celkovou implementací GDPR, ale pouze doplněním požadavků vztahujících se ke kamerovému systému.

Projekt bude probíhat v několika základních krocích:

- revize záznamů o činnostech zpracování,
- GAP analýza,
- aplikace požadavků GDPR,
- návrh kamerového systému,
- DPIA analýza,
- aplikace požadovaných úprav.

Podrobnější popis jednotlivých činností projektu se nachází níže v dalších kapitolách.

Všechny náklady na projekt bude hradit škola. Veškeré požadavky na zabezpečení osobních údajů, které budou v rámci projektu řešeny, vycházejí z Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (Obecné nařízení o ochraně osobních údajů).

Management projektu

Projekt navrhuje Anna Vaňková s využitím odborných konzultací poskytovaných panem Pavlem Říhou, který se zabývá návrhy kamerových systémů a oblastí GDPR.

V případě realizace samotného projektu zavedení kamerového systému a s tím souvisejících požadavků GDPR, bude projekt řídit pan Pavel Říha. Zavedení kamerového systému bude provedeno externí firmou, kterou může být například firma TINT s.r.o. Do realizace projektu bude také zapojen správce a někteří zpracovatelé osobních údajů v organizaci (např. pracovník IT).

Technické a technologické aspekty projektu

Nově požadovaný kamerový systém bude navržen tak, aby byly záznamy z kamer ukládány na síťové uložiště, které by mělo být umístěno v datovém rozvaděči. Datový rozvaděč je trvale uzamčen a fyzický přístup k němu má pouze omezený počet lidí. Přístupy ke kamerovým záznamům budou mít také pouze vybraní zaměstnanci školy. Mimo jiné by měl systém také automaticky zaznamenávat a ukládat veškerá přihlášení a případné změny, které by byly s nahrávkami provedeny. To je důležité opatření pro případ neoprávněné manipulace, kdy bude možné zpětně dohledat, kdo z pověřených zaměstnanců tuto manipulaci prováděl.

Samotný datový rozvaděč je umístěn v jedné z učeben, a i přesto, že je trvale uzamčen, je volně přístupný všem žákům a zaměstnancům školy, což může představovat riziko pro ochranu ukládaných dat. Avšak s ohledem na charakter místnosti zde nelze umístit kameru pro ochranu datového rozvaděče.

Jednotlivé kamery budou nastaveny tak, aby nahrávaly pouze při detekci pohybu, díky čemuž dojde k zamezení zaplňování datového uložiště nepotřebnými záznamy. Dále budou kamery snímající dveře kanceláří nastaveny tak, aby nepořizovaly záznamy ve všedních dnech v době od 8:00 do 13:00. Důvodem tohoto opatření je snaha zabránit hrozbě nahrávání pracovního prostoru zaměstnanců, v případě že by dveře kanceláře zůstaly otevřené. Takovéto nahrávání není přípustné.

Doba uložení kamerových záznamů bude nastavena maximálně na dobu sedmi dnů. Po uplynutí této doby budou záznamy automaticky odstraněny. Toto opatření zajistí možnost dohledání kamerového záznamu v případě potřeby prokázání pachatele trestného činu či přestupku, a současně nezpůsobí nepřiměřený zásah do soukromí v podobě příliš dlouhé doby ukládání záznamů. Jelikož se jedná o docela krátkou dobu ukládání záznamů, snižuje se tím také riziko jejich zneužití.

Způsob zajištění projektu

U projektů implementace požadavků GDPR existují obecně tři možné přístupy. První variantou je, že si vedení organizace zvolí svého zástupce, který bude vykonávat roli projektového manažera, sám si všechna pravidla a požadavky GDPR nastuduje, případně absolvuje školení a následně bude samotnou implementaci organizovat a řídit. V tomto případě je důležité zdůraznit, že by tuto funkci neměl vykonávat pověřenec pro ochranu osobních údajů, který by měl zastávat spíše funkci konzultanta a do samotného procesu implementace se aktivně nezapojovat. Tato varianta je možná ze všeho nejlevnější, avšak nejvíce riziková a nejnáročnější z časového hlediska.

Druhou variantou je zavádění GDPR v organizaci s pomocí firmy či alespoň konzultanta, který se na tuto oblast specializuje a celý proces bude řídit. U této varianty je nejdůležitější zvolit kvalitního konzultanta, a také to, aby se celá organizace aktivně do procesu zapojila. V tomto případě se nejspíše jedná o nejdražší, avšak nejefektivnější variantu minimalizující rizika nesouladu s GDPR.

Poslední možností je využití speciálního software, který pověřené osoby v dané organizaci provede implementací krok za krokem. Nevýhodou tohoto řešení může být to, že program nemusí být stoprocentně přizpůsoben požadavkům firmy, jako v případě využití externích konzultantů. Jako příklad takového programu lze uvést aplikaci xGDPR od české společnosti 4Stars, s.r.o.

V případě projektu řešeného v této diplomové práci je využita druhá varianta implementace požadavků GDPR, kdy je projekt zpracováván ve spolupráci s odborným konzultantem na oblast GDPR.

Náklady projektu

Přibližné celkové náklady na projekt jsou zachyceny v tabulce 5.1.

Tabulka 5.1 Odhadované náklady projektu (zdroj: vlastní zpracování)

Popis	Počet	Cena/ks	Cena celkem
Kamerové zkoušky	1	9 600,00 Kč	9 600,00 Kč
Kamery – celkem 11 kusů, typ dle výsledku kamerové zkoušky	1	187 000,00 Kč	187 000,00 Kč
Server/PC pro kamerový systém včetně datového úložiště	1	55 000,00 Kč	55 000,00 Kč
Instalační materiál (kabely, konektory, instalační lišty, PoE Switch pro kamery)	1	48 000,00 Kč	48 000,00 Kč
Software pro správu kamer a práci se záznamem (vč. Kamerových licencí)	1	36 000,00 Kč	36 000,00 Kč
Montážní práce (instalace kamer a kabeláže)	1	32 000,00 Kč	32 000,00 Kč
Dokumentace skutečného stavu a řízení projektu	1	16 000,00 Kč	16 000,00 Kč
Návrh interní směrnice kamerového systému dle požadavků GDPR	1	6 400,00 Kč	6 400,00 Kč
Cena bez DPH			**390 000,00 Kč**

Po připočítání DPH se předběžné náklady na projekt dostanou na částku 471 900,00 Kč. V případě zapojení konzultanta na GDPR do realizace projektu je potřeba počítat s dalším navýšením nákladů. Předběžný časový odhad zapojení konzultanta do projektu je 70 hodin. V takovém případě by se náklady na toho pracovníka pohybovaly okolo 42 000,00 Kč.

U prvotní implementace GDPR v organizaci by se náklady projektu určitě zvýšily o náklady na školení zaměstnanců, které se podle serveru gdpr.cz může pohybovat okolo 33 000,00 Kč. Doba zapojení externího konzultanta by se také prodloužila minimálně na dvojnásobek. V případě vypracování návrhu požadovaných dokumentů externí organizací náklady dále porostou. Základní balíček vzorových dokumentů pro implementaci GDPR je k zakoupení na webu www.gdpr.cz za cenu 7 500,00 Kč. Cena balíčku obsahující veškeré potřebné vzorové dokumenty je 19 500,00 Kč.

Harmonogram realizace projektu

Konkrétní časový harmonogram projektu je v současné době velmi obtížné určit, jelikož ještě není provedena plánovaná rekonstrukce školy, která je naplánována na období prázdnin, aby nebyla narušena výuka na škole. Teprve po dokončení této rekonstrukce může škola začít zavádět kamerový systém a s tím související implementaci požadavků GDPR.

Vzhledem k dosti finančně náročné realizaci obou projektů je velmi pravděpodobné, že se realizace zavádění kamerového systému uskuteční až příští rok. V tom případě by ideálním obdobím pro realizaci toho projektu byly opět letní prázdniny. V ideálním případě by měl být projekt ukončen před začátkem dalšího školního roku. Podrobnější časový plán jednotlivých aktivit je zachycen v tabulce WBS.

Řízení rizik projektu

Hlavní rizika spojená s realizací tohoto projektu souvisejí právě s ochranou osobních údajů. K hodnocení rizik kamerového systému na ochranu osobních údajů podle GDPR slouží analýza DPIA.

Dalším organizačním, technologickým a implementačním rizikům v projektu lze docela dobře předcházet pečlivým zmapováním současné situace a detailním naplánováním projektu a všech jeho nezbytných kroků.

5.1.2 Struktura činností projektu

Důležitým krokem před zahájením prací na projektu je stanovení činností, které budou muset být vykonány. Zároveň je dobré stanovit dobu trvání jednotlivých činností pro vytvoření základní představy o době trvání projektu. K tomuto účelu může být využit například softwarový nástroj MS Project.

Gymnázium, pro které je projekt tvořen, se již implementací požadavků GDPR zabývalo, a tak je nutné zmapovat pouze činnosti nezbytné pro správné zavedení kamerového systému. Tento fakt výrazně sníží dobu trvání hlavně při tvorbě GAP analýzy, která již nebude muset být provedena tak důkladně, jako při první implementaci GDPR.

Tabulka WBS zpracovaná pro projekt implementace požadavků GDPR v souvislosti se zaváděním kamerového systému na gymnáziu, která byla vypracována v programu MS Project, je zachycena na obrázku 5.1. Z tohoto obrázku lze vyčíst, že projekt je rozdělen do třech základních fází – fáze přípravy, fáze mapování a fáze implementace. V tabulce jsou

zachyceny nejdůležitější odhadované kroky, které bude potřeba při implementaci podniknout. Při realizaci projektu se samozřejmě některé podniknuté kroky mohou lišit, a tak bude zapotřebí tabulku průběžně aktualizovat. Největší změny v činnostech nejspíše nastanou ve fázi realizace, kde mohou být po provedení GAP analýzy zjištěny další nezbytné kroky implementace GDPR v organizaci.

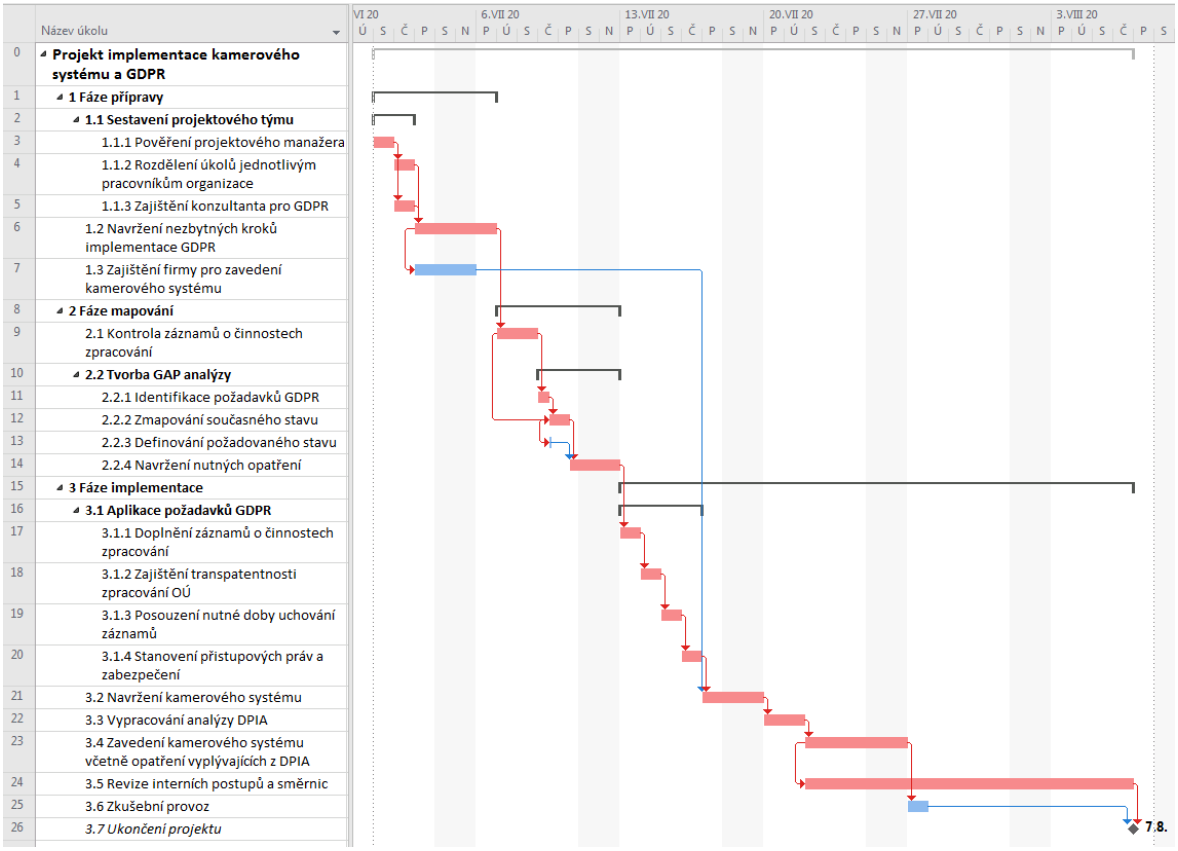
	Název úkolu	Doba trvání	Zahájení	Dokončení	Následníci
0	**Projekt implementace kamerového systému a GDPR**	**27 dny**	**1.7. 20**	**7.8. 20**	
1	**1 Fáze přípravy**	**4 dny**	**1.7. 20**	**7.7. 20**	
2	**1.1 Sestavení projektového týmu**	**2 dny**	**1.7. 20**	**3.7. 20**	
3	1.1.1 Pověření projektového manažera	1 den	1.7. 20	2.7. 20	4;5
4	1.1.2 Rozdělení úkolů jednotlivým pracovníkům organizace	1 den	2.7. 20	3.7. 20	6
5	1.1.3 Zajištění konzultanta pro GDPR	1 den	2.7. 20	3.7. 20	6
6	1.2 Navržení nezbytných kroků implementace GDPR	2 dny	3.7. 20	7.7. 20	7SS;9
7	1.3 Zajištění firmy pro zavedení kamerového systému	1 den	3.7. 20	6.7. 20	21
8	**2 Fáze mapování**	**4 dny**	**7.7. 20**	**13.7. 20**	
9	2.1 Kontrola záznamů o činnostech zpracování	2 dny	7.7. 20	9.7. 20	11;12SS
10	**2.2 Tvorba GAP analýzy**	**2 dny**	**9.7. 20**	**13.7. 20**	
11	2.2.1 Identifikace požadavků GDPR	4 hodin	9.7. 20	9.7. 20	12
12	2.2.2 Zmapování současného stavu	8 hodin	9.7. 20	10.7. 20	13SS;14
13	2.2.3 Definování požadovaného stavu	2 hodin	9.7. 20	9.7. 20	14
14	2.2.4 Navržení nutných opatření	4 hodin	10.7. 20	13.7. 20	17
15	**3 Fáze implementace**	**19 dny**	**13.7. 20**	**7.8. 20**	
16	**3.1 Aplikace požadavků GDPR**	**4 dny**	**13.7. 20**	**17.7. 20**	
17	3.1.1 Doplnění záznamů o činnostech zpracování	1 den	13.7. 20	14.7. 20	18
18	3.1.2 Zajištění transpatentnosti zpracování OÚ	1 den	14.7. 20	15.7. 20	19
19	3.1.3 Posouzení nutné doby uchování záznamů	1 den	15.7. 20	16.7. 20	20
20	3.1.4 Stanovení přístupových práv a zabezpečení	1 den	16.7. 20	17.7. 20	21
21	3.2 Navržení kamerového systému	1 den	17.7. 20	20.7. 20	22
22	3.3 Vypracování analýzy DPIA	2 dny	20.7. 20	22.7. 20	23
23	3.4 Zavedení kamerového systému včetně opatření vyplývajících z DPIA	3 dny	22.7. 20	27.7. 20	24SS;25
24	3.5 Revize interních postupů a směrnic	12 dny	22.7. 20	7.8. 20	26
25	3.6 Zkušební provoz	1 den	27.7. 20	28.7. 20	26
26	*3.7 Ukončení projektu*	*0 dny*	*7.8. 20*	*7.8. 20*	

Obrázek 5.1 WBS implementace GDPR pro kamerový systém (zdroj: vlastní zpracování)

Společně s činnostmi projektu byly navrženy také doby jejich trvání. Je důležité zdůraznit, že se jedná pouze o hrubý odhad, avšak i tyto doby byly konzultovány s odborníkem na oblast GDPR a kamerové systémy a byly odhadovány na základě jeho předchozích zkušeností. Tyto doby trvání jsou odhadnuty pro situaci, že se škola rozhodne většinu prací spojených s implementací požadavků GDPR provádět sama a konzultanta pro oblast GDPR využije pouze minimálně, spíše jen pro ověření, že bylo vše vykonáno správně.

Vzhledem k tomu, že před realizací toho projektu je potřeba nejprve provést rekonstrukci školy, která je naplánovaná na letní prázdniny, je předpokládané zahájení realizace tohoto projektu na začátku prázdnin příštího roku.

Při současném rozvržení činností projektu si lze všimnout, že jednotlivé činnosti na sebe často navazují a nemají stanoveny žádné rezervy, čímž se stávají kritickými a opožděním jakékoliv činnosti bude opožděn celý projekt. Pro lepší znázornění jsou činnosti projektu zachyceny pomocí Ganttova diagramu na obrázku 5.2.



Obrázek 5.2 Ganttův diagram implementace GDPR pro kamerový systém (zdroj: vlastní zpracování)

Tuto situaci je možné do jisté míry zlepšit zapojením většího počtu lidí a paralelizací některých činností. Ve většině případů je však začátek každé činnosti podmíněn ukončením té předcházející (jedná se o projekt typu Vodopád).

Z tabulky WBS je však také možné vyčíst, že celkový odhad doby trvání projektu je stanoven na 27 dní a v případě, že nebude žádná z činností zpožděna, může být projekt ukončen do 7.8. Je nezbytné si uvědomit, že v tom případě by do konce prázdnin, kdy je požadováno, aby byl systém v provozu, zbývá ještě necelý měsíc. Z toho vyplývá, že případné opoždění projektu nezpůsobí výrazné potíže.

Pro obecný projekt implementace požadavků GDPR ve školské organizaci by tabulka WBS vypadala samozřejmě poněkud jinak. Pro lepší orientaci v této oblasti byla vytvořena také tabulka WBS zachycující činnosti, které je nutné provést v případě, že se škola implementací GDPR ještě nezabývala. Na rozdíl od projektu navrhovaného pro gymnázium BMA, nebyly pro jednotlivé činnosti projektu stanoveny jejich doby trvání, ani nebyl vypracován Ganttův diagram. K tomuto rozhodnutí došlo z důvodu možných velkých rozdílností těchto údajů v závislosti na velikosti organizace, na jejím dosavadním nakládání s osobními údaji a také na možnosti zapojení interních či externích zdrojů. Lze však říci, že největší časový rozdíl u obecné implementace GDPR ve školách oproti projektu řešenému pro gymnázium bude u fáze analyzování procesů, při nichž dochází ke zpracování osobních údajů, která již u gymnázia byla provedena dříve a nyní ji bylo možno zcela vynechat.

Další podstatný časový rozdíl bude u GAP analýzy. V případě gymnázia byl časový odhad této analýzy stanoven na 2 pracovní dny neboli 16 hodin. U obecné prvotní implementace GDPR by tato doba byla podstatně vyšší a mohla by se pohybovat okolo 80 hodin. Následné zajištění souladu s GAP analýzou by bylo také časově náročnější a mohlo by se pohybovat až okolo 200 hodin. Z toho důvodu je nutné si pro takový projekt vyhradit dostatečné množství času.

Nutné zapojení externího konzultanta je v takovém případě odhadnuto na 134 hodin, což se následně projeví také v nákladech projektu. Tabulka WBS zachycující základní kroky prvotní implementace požadavků GDPR ve školské organizaci se nachází na obrázku 5.3.

	Název úkolu
0	**Projekt implementace GDPR**
1	**1 Fáze přípravy**
2	1.1 Zajištění školení zaměstnanců
3	**1.2 Rozdělení projektových prací**
4	1.2.1 Identifikace zpracovatelů a správce
5	1.2.2 Stanovení projektového manažera
6	1.2.3 Zajištění konzultanta GDPR
7	**1.3 Zajištění DPO**
8	1.3.1 Ověření nutnosti jmenování DPO
9	1.3.2 Výběr vhodného kandidáta
10	1.3.3 Jmenování DPO
11	**2 Fáze mapování**
12	**2.1 Provedení analýzy procesů zpracování OÚ**
13	2.1.1 Zmapování účelů zpracování OÚ
14	2.1.2 Identifikace subjektů údajů
15	2.1.3 Určení typů osobních údajů
16	2.1.4 Ověření zákonnosti zpracování
17	2.1.5 Vytvoření karty záznamů o činnostech zpracování
18	**2.2 Provedení GAP analýzy**
19	2.2.1 Identifikace požadavků GDPR
20	2.2.2 Zmapování současného stavu
21	2.2.3 Definování požadovaného stavu
22	2.2.4 Navržení nutných opatření
23	**3 Fáze implementace**
24	**3.1 Aplikace požadavků GDPR**
25	3.1.1 Doplnění zpracovatelských smluv
26	3.1.2 Revize formulářů a smluv pro zaměstnance
27	3.1.3 Revize formulářů a smluv pro studenty
28	3.1.4 Vypracování souhlasů o zpracování OÚ
29	3.1.5 Zajištění transparentnosti zpracování OÚ
30	3.1.6 Vypracování nutných DPIA analýz
31	**3.2 Navržení formy zabezpečení OÚ**
32	3.2.1 Stanovení zabezpečení HW
33	3.2.2 Stanovení zabezpečení SW
34	3.2.3 Stanovení zabezpečení fyzických dokumentů
35	3.2.4 Stanovení přístupových práv
36	3.2.5 Aplikace vybrané formy zabezpečení
37	**3.3 Revize interních postupů a směrnic**
38	3.3.1 Popis postupů pro zpracování OÚ
39	3.3.2 Popis pravidel zabezpeční OÚ
40	3.3.3 Návrh evidence souhlasů o zpracování OÚ
41	3.3.4 Návrh evidence požadavků subjektů údajů
42	3.3.5 Návrh evidence školení
43	3.3.6 Navržení postupů řešení bezpečnostních incidentů
44	3.3.7 Návrh evidence bezpečnostních incidentů
45	3.3.8 Uprava webových stránek
46	**3.4 Vedení deníku implementace GDPR**

Obrázek 5.3 WBS obecné implementace GDPR (zdroj: vlastní zpracování)

5.2 Analýza procesů zpracování dat

Analyzování procesů zpracování dat a vypracování karty záznamů o činnostech je ve většině případů nejnáročnější a nejzdlouhavější částí implementace požadavků GDPR. U velkých organizací tato analýza může trvat několik dnů až týdnů. Z organizačního hlediska by měl být do procesu zpracování analýzy zapojen každý, kdo v rámci organizace pracuje s osobními údaji. Úkolem těchto lidí by mělo být provedení detailního popisu jaká data a za jakým účelem zpracovávají, včetně doplnění dalších informací potřebných ke správnému vypracování karty záznamů o činnostech. Dále by měl být stanoven projektový manažer, který by analýzu činností řídil a sestavoval zmiňovanou kartu záznamů o činnostech. Může se jednat o specialistu v oblasti GDPR, který není zaměstnancem organizace, a tak má při zpracování analýzy potřebný nadhled. Levnější variantou je pověřit do této funkce interního zaměstnance a externistu využívat pouze v případě nutných konzultací. Nápomocen by mu měl být správce, nesoucí odpovědnost za správné vypracování, a případně také pověřenec pro ochranu osobních údajů. Proto je dobré se zabývat jmenováním DPO hned na začátku procesu implementace GDPR, jak to bylo zachyceno již v tabulce WBS (obrázek 5.4).

Jelikož to již bude rok, co vešlo Obecné nařízení v platnost, lze očekávat, že škola bude mít již základní požadavky GDPR implementovány. V tom případě musí mít také vedeny záznamy o činnostech zpracování osobních údajů. Stále však existují instituce, které nemají požadavky GDPR implementovány, nebo je mají implementovány nesprávně. Z toho důvodu byla jako součást této diplomové práce vytvořena vzorová karta záznamů o činnostech obsahující základní procesy zpracování osobních údajů, které se ve škole obecně provádí. Karta záznamů o činnostech, kterou již má škola zpracovanou, bude se vzorovou kartou porovnána a doplněna tak, aby byla přehledná a zachycovala všechny důležité položky. Vzorová karta záznamů o činnostech se nachází v příloze 2 této práce a pro své účely ji mohou využít (a upravit podle svých potřeb) také další školské právnické osoby.

5.3 GAP analýza

Základním krokem pro správnou implementaci všech požadavků nařízení GDPR je provedení GAP analýzy, která zachycuje rozdíly mezi aktuálním stavem a stavem požadovaným.

Největší problém, který vniká v souvislosti s tvorbou této analýzy, je stanovení, jak má analýza vypadat a co všechno má obsahovat. Na základě výše uvedeného byl vytvořen prázdný návrh této analýzy zachycující základní požadavky vyplývající z Obecného nařízení, které musí být v organizacích aplikovány. Vzor, podle něhož může být GAP analýza přehledně vypracována, zachycuje tabulka 5.2.

Tabulka 5.2 GAP analýza (zdroj: vlastní zpracování)

Požadavky GDPR	**Současný stav**	**Požadovaný stav**	**Nutná opatření**
Vedení záznamů o činnostech zpracování (včetně všech potřebných informací)			
Dodržování zákonnosti zpracování			
Zajištění transparentnosti zpracování			
Zajištění důvěryhodnosti zpracovatelů			
Vedení evidence zpracovatelských smluv			
Jmenování DPO			
Zabezpečení osobních údajů			
Zpracování potřebných analýz DPIA			
Vedení evidence bezpečnostních incidentů a porušení Obecného nařízení			
Vedení evidence požadavků subjektů údajů o naplnění práv			
Vedení evidence udělených souhlasů			
Školení zaměstnanců v oblasti GDPR			
Revize pracovních postupů a interních směrnic			
Zajištění předávání osobních údajů do zahraničí			

Prvním požadavkem zachyceným v analýze je správné vypracování záznamů o činnostech zpracování osobních údajů. K tomu je ve školských organizacích vhodné využít vypracovanou vzorovou kartu záznamů o činnostech, zachycující všechny nezbytné informace. V souvislosti s plánovaným zavedením kamerového systému ve škole BMA je nutné doplnit záznamy o činnostech, o záznam zpracování osobních údajů s tímto spojený.

Na záznamy o činnostech zpracování úzce navazuje kontrola, zda je každé toto zpracování zákonně podloženo. Podmínky zákonnosti zpracování byly vypsány v kapitole 2.2. Jestliže některé zpracování není zákonné, musí být osobní údaje s tím spojené buďto vymazány, nebo musí být v co jak nejkratší době doloženy souhlasy o zpracování údajů, které budou podepsané subjekty údajů, jichž se toto zpracování týká.

Obecné nařízení vyžaduje, aby každé zpracování osobních údajů bylo transparentní, což znamená, že instituce netají, jaké osobní údaje zpracovává. Toho může být dosaženo například uveřejněním základních informací o zpracování osobních údajů na webu instituce, včetně kontaktních údajů na osoby odpovídající za zpracování.

Dalším požadavkem vyplývajícím z nařízení GDPR je povinnost správce zajistit, aby zpracovatelé byli důvěryhodné osoby, což by měl být správce schopen nějakým způsobem doložit.

S tímto je úzce spojen další bod GAP analýzy, a to je kontrola, zda je s každým zpracovatelem uzavřena smlouva o zpracování. Tato smlouva musí odpovědět na otázky co, jak, jak dlouho a za jakým účelem bude zpracovatel zpracovávat. Mimo to by měla obsahovat také práva a povinnosti správce údajů. Osoba, se kterou správce neuzavřel tuto smlouvu, není oprávněna osobní údaje zpracovávat.

Následně je nutné ověřit, zda instituce musí mít pověřence pro ochranu osobních údajů a v případě že ano, musí zajistit dostatečně kvalifikovanou osobu pro tuto funkci. Jak již bylo dříve zmíněno, každá škola pověřence mít musí. Zbývá tedy zajistit tu správnou a dostatečně kvalifikovanou osobu. Škola BMA má jako pověřence pro ochranu osobních údajů externího pracovníka, jehož kontaktní údaje lze nalézt na webu školy.

Jedním z nejdůležitějších kroků, které je nutné provést, je kontrola zabezpečení osobních údajů. Správce a zpracovatelé musí podle Obecného nařízení provést taková vhodná opatření, aby byla zajištěna důvěrnost, integrita a dostupnost údajů. Zabezpečení by mělo odpovídat hrozícím rizikům a mělo by být pravidelně kontrolováno a testováno. Zajištěno musí být zabezpečení jak organizační, tak technické. Fyzické dokumenty

obsahující osobní údaje (například třídní knihy či osobní složky studentů) by měly být uschovány v uzamykatelných skříních, do nichž by měly mít přístup pouze oprávněné osoby. Nutné je také dostatečně zabezpečit osobní údaje v elektronické podobě. Efektivního zabezpečení údajů lze dosáhnout například pomocí zavedení systému bezpečnosti informací (ISMS). Postup zavádění ISMS je popsán pomocí norem ISO/IEC 27001 a ISO/EIC 27002.

Na základě záznamů o činnostech zpracování musí být vyhodnoceno, zda je některý z procesů zpracovávání osobních údajů rizikový a vyžaduje provedení posouzení vlivu na ochranu osobních údajů. Jestliže ano, a DPIA analýza pro tento proces ještě nebyla vypracována, je potřeba to napravit. V případě školy BMA prozatím k žádnému zpracování údajů vyžadující analýzu DPIA nedocházelo, avšak při zavádění kamerového systému bude vypracování této analýzy nezbytné.

Jestliže někdy došlo k bezpečnostním incidentům souvisejícím s ohrožením osobních údajů, je potřebné vést evidenci těchto incidentů, ať už pro potřeby subjektů údajů nebo kvůli kontroly dozorového orgánu.

V případě, že subjekt údajů uplatňuje svá práva vztahující se k osobním údajům, měla by instituce mít tyto případy evidovány. Evidence slouží hlavně pro potřeby instituce, a to například kvůli doložení oprávněnosti zaúčtování poplatků za opakované (nepřiměřené) žádosti subjektů údajů na uplatňování svých práv. Je to také obranný mechanismus pro potřebu doložení naplnění práv subjektů údajů v případě výskytu nedorozumění. Doporučuje se, aby součástí těchto záznamů byl podpis subjektu údajů, který se svých práv dožadoval.

Dalšími dokumenty, které musí být nutně evidovány, jsou souhlasy o zpracování osobních údajů od všech osob, od nichž jsou tyto souhlasy vyžadovány. Uchovávání souhlasů je důležité pro potvrzení zákonnosti zpracovávání údajů, a proto je nezbytné ověřit, zda žádný souhlas nechybí a vše je evidováno v přehledné formě. Současně by mělo být ověřeno, zda jsou souhlasy správně zpracovány, aby byly srozumitelné a svobodné. Důležité je pamatovat také na to, že souhlas by měl být až poslední možností, jestliže neexistuje žádný jiný zákonný důvod zpracování osobních údajů.

Každý zaměstnanec instituce je povinen absolvovat školení týkající se ochrany osobních údajů a nových povinností souvisejících s nařízením GDPR. V rámci GAP analýzy je dobré ověřit, zda byli opravdu proškoleni všichni zaměstnanci a jestli se v dané

problematice dostatečně orientují. Měl by také existovat dokument pro ověření účasti na školeních.

Jednou z nejdůležitějších a nejpracnějších oblastí GAP analýzy je kontrola interních postupů a směrnic. Tyto dokumenty musí být zpracovány tak, aby nastavovaly pravidla v organizaci v souladu s GDPR. Jejich součástí by mělo být vymezení, kdo má k jednotlivým osobním údajům přístup a za jakých okolností. Dále by interní dokumenty měly obsahovat způsob zabezpečení údajů a postup pro jejich zpracovávání. Důležité je také správné vypracování formulářů, dotazníků a smluv tak, aby byly po subjektech údajů vyžadovány jen nezbytné informace.

Posledním bodem ve výše zmiňované analýze je zajištění předávání osobních údajů do zahraničí. Toto předávání může být uskutečněno, jestliže země zajišťuje dostatečnou úroveň ochrany, předávání je založeno na vhodných zárukách nebo jsou splněny jiné podmínky vyjmenované v Obecném nařízení. Jelikož škola BMA údaje do zahraničí nepředává, nemusí se o tuto oblast více zajímat.

Po zmapování výše uvedených oblastí a navržení nutných změn je potřeba tyto změny implementovat. Je důležité zmínit, že jednotlivé požadavky zmiňované v GAP analýze nejsou zdaleka vyčerpávající a jedná se pouze o výčet základních oblastí, na které je potřeba se zaměřit. Požadavky uváděné v analýze by měly být dále rozloženy na menší oblasti, až po kontrolu jednotlivých činností souvisejících s GDPR.

Provedení GAP analýzy v organizaci, která se implementací požadavků GDPR ještě více nezajímala, je časově dosti náročný proces. Stejně jako u analýzy zpracovávání osobních údajů se může jednat o dny či týdny, podle velikosti organizace. Do zpracování GAP analýzy by se měli zapojit hlavně projektový manažer, správce, pověřenec pro ochranu osobních údajů a pracovník IT, který má na starosti zabezpečení počítačové sítě.

5.3.1 GAP analýza ve školském zařízení

Ve škole BMA byla důkladná GAP analýza již provedena při prvotním zavádění požadavků GDPR, a tak jí není nutné vypracovávat celou znovu. Měly by však být zmapovány oblasti, které budou dotčeny při zavádění kamerového systému.

Karta záznamů o činnostech musí být doplněna o zpracování osobních údajů souvisejících s monitorováním prostorů školy. Je důležité předem jasně stanovit, k čemu budou kamerové záznamy sloužit, kdo a za jakých okolností k nim bude mít přístup, jak

dlouho budou záznamy uchovávány, a také kde budou uchovávány. Kvůli transparentnosti zpracování osobních údajů musí být na viditelném místě umístěna informace o snímání prostor kamerovým systémem.

Před samotným zavedením kamer musí být vypracován návrh jejich umístění tak, aby bylo pokryto vše potřebné, ale současně musí být kladen důraz na požadavky GDPR. Následně musí být pro kamerový systém vypracována analýza DPIA a navrženy případné úpravy. Současně je důležité navrhnout dostatečné zabezpečení kamerových záznamů a místa, kde budou tyto záznamy uloženy.

Posledním nutným krokem pro správnou implementaci požadavků GDPR – při zavádění kamerového systému – je na základě GAP a DPIA analýz vypracování interní směrnice pro tento kamerový systém. Tato směrnice by měla především zachycovat zabezpečení kamerového systému, oprávnění pracovníků na přístup k záznamům, a také dobu ukládání kamerových záznamů.

5.4 Návrh kamerového systému se záznamem

Pro správné navržení projektu implementace požadavků GDPR spojených se zaváděním kamerového systému ve škole, je nezbytným krokem samotné navržení kamerového systému. Z tohoto návrhu bude následně vycházet analýza DPIA, která také posoudí, zda není nutné návrh kamerového systému pozměnit.

Samotný návrh kamerového systému byl vypracován ve spolupráci s panem Pavlem Říhou, který se touto oblastí zabývá a pravděpodobně se bude podílet také na případné realizaci projektu.

Jak již bylo naznačeno ve studii proveditelnosti projektu, návrh kamerového systému popisuje umístění jedenácti kamer a je více rozepsán v následujícím textu.

Přesnější umístění a nastavení jednotlivých kamer bude upřesněno při případné realizaci projektu. Ještě jednou je potřeba zmínit, že žádná z kamer by neměla zachycovat toalety. Všechny kamery umístěné v nadzemních podlažích budou tedy nastaveny tak, aby vždy jedna ze dvou kamer zachycovala pouze prostory schodiště a ta druhá bude zaznamenávat oblast na opačnou stranu, tj. od toalet směrem ke dveřím kanceláří.

Součástí návrhu kamerového systému, je také grafické zobrazení umístění kamer na třech současných podlažích budovy. Obrázky s těmito návrhy lze zalézt v příloze číslo.

Kamera číslo 1 – hlavní vchod, přízemí

První kamera by měla být umístěna v zádveří tak, aby snímek z kamery zajistil dostatečně detailní obraz každé vstupující osoby. Tím bude zajištěna možnost snadné identifikace každé osoby, která by do prostor školy vstoupila neoprávněně. Zároveň by tato kamera umožňovala pracovníkovi na sekretariátu školy kontrolu nad tím, komu druhé vstupní dveře otevírá. V současnosti je k tomuto účelu používána stávající kamera na chodbě, která však neposkytuje žádné detailní informace a ani nepořizuje záznamy.

Účelem této kamery je zamezit neoprávněnému vstupu do budovy, a také pořídit důkazní materiály v případě pokusu o násilné vniknutí. Jelikož se bude kamera nacházet v prostoru, který je veřejně přístupný, doporučuje se použít kameru typu kopule se zvýšenou mechanickou odolností, která zajistí větší ochranu před rozbitím či vychýlením z nastaveného záběru.

Kamera číslo 2 – šatny, přízemí

Druhá kamera by měla být umístěna ve vstupní hale a měla by být nasměrována směrem k šatním skříňkám a na okna. Hlavním účelem této kamery je kontrola prostoru šaten pro snížení drobné kriminality (vykradení šatních skříněk). Mimo to kamera zajišťuje důkazní materiál v případě násilného vniknutí do budovy oknem.

Kamera číslo 3 – schodiště, přízemí

Třetí kamera by měla být umístěna ve vstupní hale, kde by monitorovala prostor od schodiště až po vstup do školní jídelny, který je využíván studenty a zaměstnanci školy. Sledování tohoto vstupu do školní jídelny je velmi důležité, protože ze strany jídelny neexistuje v tuto chvíli žádné zabezpečení ani žádný způsob kontroly vchodu, a v současné době je možné se přes jídelnu nepozorovaně a bez oprávnění dostat do budovy. Zachycením všech vstupujících osob do prostorů školy z jídelny se zvyšuje šance následné identifikace případného pachatele trestné činnosti či drobné kriminality.

Součástí záběru kamery by měl být také vstup do multimediální učebny. Okna této učebny jsou chráněna mřížemi a dveře, které budou zachycené na kameře, jsou jediným možným vstupem do místnosti. Tímto opatřením bude zajištěna ochrana všech technologií v učebně. V případě pokusu o krádež bude pachatel zachycen na záznamu kamery jak při vstupu, tak při odchodu z učebny.

Kamera číslo 4 – schodiště, 1. nadzemní patro

Čtvrtá kamera by měla být umístěna nad dveřmi do kanceláře sekretariátu školy a měla by sledovat prostor směrem ke schodišti. Na záběru z kamery budou také vstupy do jednotlivých učeben vlevo, až po schodiště. Kamera bude určena převážně pro kontrolu pohybu osob po budově a jejich vstup do učeben na tomto patře.

Kamera číslo 5 – kanceláře, 1. nadzemní patro

Pátá kamera by měla být umístěna na stěně u oken a měla by být namířena směrem od toalet ke dveřím kanceláří ředitele a sekretariátu. Obě tyto kanceláře jsou obzvláště důležité, nejen pro ochranu osobních údajů. Jejich ochrana je mimo jiné klíčová pro splnění požadavků stanovených Obecným nařízením.

Kamera číslo 6 – schodiště, 2. nadzemní patro

Šestá kamera by měla být umístěna nad dveřmi do kanceláře nacházející se v patře nad sekretariátem a měla by sledovat prostor směrem ke schodišti, stejně jako kamera v prvním nadzemním podlaží budovy. Na záběru z kamery by rovněž měly být vstupy do jednotlivých učeben vlevo, až po schodiště. V prostřední z těchto učeben je umístěn datový rozvaděč se serverem a datovým uložištěm. Tento fakt zvyšuje význam kamery, která by měla alespoň z části zajišťovat ochranu datového rozvaděče.

V případě, že dojde k neoprávněnému zásahu do datového rozvaděče v provozní době školy, nebude možné určit kdo tento zásah způsobil. Jestliže však dojde mimo provozní dobu školy k neoprávněnému vniknutí do budovy, může záznam z kamery sloužit jako důkaz o tom, zda byl pachatel v prostoru rozvaděče či ne.

Kamera číslo 7 – kanceláře, 2. nadzemní patro

Sedmá kamera by měla být umístěna na stěně u oken a měla by být namířena směrem od toalet k jednotlivým dveřím od kabinetů vyučujících. Kamera bude sloužit především pro zajišťování důkazních materiálů v případě, že dojde k vandalismu nebo krádeži.

Kamera číslo 8 – schodiště, 3. nadzemní patro

Osmá kamera by se měla nacházet v plánovaném 3. nadzemním patře, které teprve bude vystavěno. Tato kamera by měla být umístěna nad dveřmi kanceláře, která se bude v rámci patra nacházet na stejném místě jako sekretariát ležící o dvě patra níže a měla by sledovat prostor směrem ke schodišti, kde se vlevo budou nacházet vstupy do učeben, stejně

jako u předchozích dvou pater. Kamera bude sloužit především pro monitorování pohybu osob po budově a jejich vstup do učeben na tomto patře.

Kamera číslo 9 – kanceláře, 3. nadzemní patro

Další kamera by se měla nacházet na stěně u oken připravovaného nového patra. Opět by měla být namířena směrem od toalet ke kabinetům vyučujících. Účelem této kamery bude zajišťování důkazních materiálu v případě, že dojde k vandalizmu nebo krádeži v některém z kabinetů.

Kamera číslo 10 – vstup na střešní terasu

Tato kamera by se měla nacházet na vnitřní straně dveří vedoucích na plánovanou střešní terasu a měla by monitorovat prostor schodiště. Hlavním účelem kamery bude identifikace všech osob vstupujících do venkovního prostoru a poskytnutí záznamu o případném neoprávněném vniknutí na střechu budovy.

Kamera číslo 11 – venkovní prostor terasy

Poslední navrhovaná kamera by se měla jako jediná nacházet ve venkovním prostoru. Z toho důvodu musí být zvolena taková kamera, která bude dostatečně odolná vůči vnějším vlivům, a tedy může být použita ve venkovním prostředí. Kamera by měla být umístěna nad vchodem na terasu a měla by monitorovat prostor této terasy, především za účelem zabránění nevhodnému chování, které by mohlo vést ke zranění či pádu ze střechy.

Při umisťování a nastavování kamery je nutné brát v úvahu okolní prostředí, a hlavně pak zamezit situacím, kdy by kamera mohla zaznamenávat okna okolních budov. V případě, že by k takovýmto situacím docházelo, tak by se jednalo o nepřiměřený zásah do soukromí třetí strany. Jestliže by nebylo možné kameru umístit a nastavit tak, aby nezachycovala okolní budovy, bylo by nutné oblast oken opatřit tzv. privátní maskou, která překryje zvolený prostor a nepořizuje z dané oblasti žádný záznam ani živý obraz.

5.5 Posouzení vlivu na ochranu osobních údajů

V souvislosti se zavedením kamerového systému ve škole bude docházet k novým případům zpracování osobních údajů, které podléhají nutnosti vypracování analýzy DPIA. Již bylo zmíněno, že formát či vzhled této analýzy není nikde striktně určen, a tak se správci při jejím zpracovávání mnohdy potýkají se značnými problémy. V současnosti existují firmy

zabývající se zpracováním Posouzení vlivu na ochranu osobních údajů, avšak v případě využití jejich služeb je nezbytné počítat se zvýšením výdajů na implementaci GDPR.

Z tohoto důvodu je jako součást práce vytvořena metodika Posouzení vlivu na ochranu osobních údajů pro stanovení míry rizika kamerových systémů. Tato metodika může být následně využita při tvorbě obdobných projektů.

5.5.1 Metodika DPIA

Metodika byla vytvořena tak, aby určovala míru rizika posuzovaného u každé kamery zvlášť. Hodnocení využívané v této metodice je založeno na metodě řízení rizik. Pro hodnocení jednotlivých kamer byly nadefinovány 4 hlavní kategorie, ve kterých musí být každá kamera zhodnocena. Tyto kategorie jsou následující:

- oprávněnost,
- zabezpečení,
- dopad,
- rozsah.

Každá z těchto kategorií má dále stanovena tři hodnotící kritéria, která jsou jednotlivě posuzována a dohromady určují hodnotu dané kategorie, za pomoci přiřazení bodů, u konkrétní kamery. Hodnoty jednotlivých kategorií se mohou pohybovat v rozsahu od 0 do 10 bodů.

Kategorie oprávněnosti a zabezpečení jsou označovány jako kladné, což znamená, že jsou u nich požadovány co nejvyšší hodnoty pro následné stanovení nižší rizikovosti kamery. Naopak kategorie dopad a rozsah jsou označovány jako záporné, a tak by stanovení vysokých hodnot u těchto kategorií naznačovalo riziko vyšší.

Celkové posouzení vlivu jednotlivých kamer na ochranu osobních údajů je rozdílem součtu hodnot kladných kategorií a součtu hodnot kategorií záporných.

$$výsledné\ hodnocení = (oprávněnost + zabezpečení) - (dopad + rozsah)$$

Každá kamera může dosáhnout v rámci posouzení vlivu výsledného hodnocení v rozsahu od -20 do 20 bodů. Stanovení významnosti rizika na základě výsledného hodnocení je zachyceno v tabulce 5.3.

Tabulka 5.3 Tabulka stanovení rizikovosti kamer (zdroj: vlastní zpracování)

	Výsledné hodnocení je rozdílem přínosů a dopadů na soukromí.
+20 až 0	žádné riziko – kamera může být použita v popsaném režimu bez rizika dopadu na soukromí
-1 až -3	nízké riziko – zvážit možné dopady, zvýšit stupeň zabezpečení, změnit úhel záběru kamery nebo přidat privátní masku
-4 až -6	střední riziko – nutno přijmout opatření. Změna nastavení kamery, zvýšení zabezpečení.
-7 až -9	vysoké riziko – nutno přijmout opatření, pokud přetrvává nutno konzultovat s dozorovým orgánem
-10 až -20	Kritické riziko – provozování kamery není oprávněné, nutno zrušit.

Oprávněnost

V této kategorii je nutné nejprve se zaměřit na právní titul zpracování osobních údajů pomocí kamerového systému (většinou se jedná o oprávněné zájmy správce) a oprávněnost konkrétní kamery k tomuto účelu. Dále musí být posouzena možnost nahrazení kamery nějakým jiným řešením, které by méně zasahovalo do soukromí subjektu údajů. Posledním hodnotícím kritériem v této kategorii je posouzení efektivnosti daného řešení společně s přínosem, který nabízí.

Výsledné hodnocení reprezentuje míru nutnosti použití této kamery před jinými technologiemi a metodami, aby bylo dosaženo maximálního možného splnění cíle. Nejvyšší možná hodnota 10 v této oblasti znamená, že oprávněný zájem je vysoký (například ochrana života) a kamera je pro daný účel nejlepším možným řešením (nebo dokonce jediným). Jestliže je naopak tato hodnota nízká, znamená to, že pro provozování kamery neexistuje dostatečný důvod, nebo lze stejného výsledku dosáhnout jinými efektivnějšími metodami, s menším dopadem na soukromí subjektů údajů.

Zabezpečení

V kategorii zabezpečení jsou hodnocena technická a organizační opatření, která mají zabránit zneužití zpracovaných osobních údajů k jiným účelům, než pro které byly původně pořízeny. Mezi tato opatření patří zejména směrnice a pracovní postupy týkající se kamerových systémů, fyzické zabezpečení datového úložiště a logické zabezpečení sítě. Například datové uložiště umístěné v uzamčené serverovně v uzamčeném datovém

rozvaděči bude poskytovat mnohem lepší fyzické zabezpečení než síťové uložiště umístěné na stole v kanceláři, do níž mají přístup všichni zaměstnanci.

Do výsledného hodnocení musí být zahrnut také počet osob oprávněných pro přístup ke kamerovým záznamům. Čím více osob má k těmto záznamům přístup, tím roste riziko neoprávněného přístupu, který může vést ke zneužití či ztrátě údajů.

Výsledné hodnocení kamery v kategorii zabezpečení s nejvyšší hodnotou 10 udává, že společnost má velmi kvalitní zabezpečení sítě a nastaveny takové postupy, že provedení útoku se záměrem odcizení dat by bylo velmi složité. Také počet zaměstnanců oprávněných přistupovat ke kamerovým záznamům je v tomto případě omezen na nejnižší možný. S každým existujícím rizikem zabezpečení výsledná hodnota v této kategorii klesá. Jestliže bude výsledná hodnota kategorie rovna 0, znamená to, že kamera ani její záznamy nejsou nijak chráněny proti zneužití.

V případě hodnocení kamerového systému ve škole BMA budou všechny kamery v této kategorii hodnoceny stejně, a to z důvodu jejich umístění na jedné datové síti se stejným přístupem. Jelikož je datový rozvaděč umístěn v učebně, která je volně přístupná všem studentům i zaměstnancům, bude mít tento fakt negativní dopad na hodnocení. Vzhledem k tomu, že se jedná pouze o návrh kamerového systému, dá se předpokládat, že při skutečné realizaci projektu, bude společností zabývající se kamerovými systémy dodána společně s kamerovým systémem také kompletní projektová dokumentace, včetně návrhu směrnice pro používání kamerového systému. Tato opatření budou mít pozitivní vliv na hodnocení v rámci kategorie zabezpečení.

Dopad

V kategorii dopadu je hodnocen především výsledný dopad systému na soukromí subjektů údajů, a to jak z hlediska intenzity zásahu do jejich soukromí, tak podle toho, o jaký druh zpracovávaných údajů se jedná. Hodnotí se, jestli kamera zabírá například detaily obličeje, jestli se jedná o nahrávku se zvukem nebo je naopak zaznamenávána pouze přehledová situace v daném prostoru. Posledním hodnoceným kritériem je kategorie zachycovaných subjektů údajů, tedy zda kamery snímají pouze omezený počet zaměstnanců, zákazníky uvnitř prodejny, nebo obecně širokou veřejnost, která má do monitorovaného prostoru přístup.

Konkrétně lze říci, že kamera umístěná uvnitř serverovny, do níž má přístup pouze omezené množství osob, bude mít podstatně nižší dopad na soukromí než kamera umístěná

na parkovišti před budovou, kam má přístup široká veřejnost. Pro lepší představu hodnocení by kamera umístěná v serverovně mohla být hodnocena v této kategorii číslem 2, zatímco kameře na parkovišti musí být přiřazena maximální hodnota 10.

Rozsah

V poslední sledované kategorii je prvním hodnotícím kritériem celkový předpokládaný počet osob, jejichž osobní údaje mají být zpracovávány. V tomto případě bude mít například kamera umístěná ve skladu, kde se pohybuje pouze několik zaměstnanců, nižší hodnocení než kamera umístěná u vstupu do prodejny, která může snímat stovky až tisíce obyvatel.

Druhým hodnotícím kritériem této kategorie je doba, po kterou budou záznamy z kamer uchovávány. Kamera, jejíž záznam bude uchováván pouze pár dnů, bude mít nižší hodnocení než kamera, jejíž záznam bude uchováván několik týdnů.

Posledním aspektem hodnocení této kategorie je režim nahrávání kamery. Kamera, která bude nahrávat nepřetržitě 24 hodin 7 dní v týdnu, bude hůře hodnocena (vyšší čísla), než kamera nahrávající pouze na základě detekce pohybu mimo pracovní dobu.

5.5.2 DPIA analýza kamerového systému

Ve spolupráci s konzultanty, zabývajícími se oblastí kamerových systémů a GDPR, byla vytvořena tabulka Posouzení vlivu na ochranu osobních údajů pro jednotlivé kamery navrhovaného kamerového systému ve škole BMA. Hodnocení jednotlivých navrhovaných kamer pomocí metodiky DPIA je zachyceno v tabulce 5.4.

Tabulka 5.4 DPIA analýza kamerového systému ve škole BMA (zdroj: vlastní zpracování)

Číslo kamery / umístění	Vnitřní / vnější	Oprávněnost	Zabezpečení	Dopad	Rozsah	Výsledné hodnocení
1- vchod	vnitřní	8	5	10	9	**-6**
2- šatny	vnitřní	7	5	9	8	**-5**
3 - schodiště 1.NP	vnitřní	7	5	8	7	**-3**
4 - schodiště 2. NP	vnitřní	6	5	8	7	**-4**
5 - kanceláře 2. NP	vnitřní	5	5	8	6	**-4**
6 - schodiště 3. NP	vnitřní	6	5	8	7	**-4**
7 - kanceláře 3. NP	vnitřní	5	5	7	6	**-3**
8 - schodiště 4. NP	vnitřní	6	5	8	7	**-4**
9 - kanceláře 4. NP	vnitřní	5	5	7	6	**-3**
10 - vchod na terasu	vnitřní	7	5	8	7	**-3**
11 - venkovní terasa	vnější	7	5	9	8	**-5**

Důležitými aspekty navrženého kamerového systému, které je nutno doplnit pro správné vypracování Posouzení vlivu na ochranu osobních údajů, jsou přístupová práva zaměstnanců a umístění datového rozvaděče. Přístup ke kamerovým záznamům by měl mít ředitel školy, sekretářka a správce IT. Datový rozvaděč, na kterém budou záznamy uloženy, je uzamčen a nachází se ve volně přístupné učebně.

Nejvyšší oprávněnost má kamera číslo 1 umístěná u vstupu do prostoru školy. Tato kamera pomáhá identifikovat neoprávněné vniknutí do školy, a také kontrolovat identitu osob, kterým jsou vzdáleně otevírány dveře do školy. V tomto případě se jedná o velmi dobré řešení pro ochranu majetku školy. Nejnižší oprávněnost mají naopak kamery monitorující dveře kanceláří učitelů. Docela vysoké hodnocení v této kategorii mají také další 2 kamery umístěné v přízemí budovy, kde je největší riziko pohybu neoprávněných osob a kamery monitorující prostor terasy, které mimo jiné slouží k zabránění incidentům ohrožujícím zdraví.

Hodnocení zabezpečení je, jak již bylo zmíněno, u všech kamer stejné, jelikož mají společné datové uložiště. Toto hodnocení není nijak vysoké, a to hlavně z důvodu, že datové uložiště se nachází ve volně přístupné místnosti, která není nijak speciálně zabezpečena. Jediným zabezpečením datového uložiště je jeho uzamykatelnost. Pro provoz kamerového systému bude nutné toto zabezpečení zvýšit.

V kategorii dopadu je nejhůře hodnocena kamera číslo 1. Tato kamera zaznamenává také oblast za prosklenými vstupními dveřmi, kde se pohybuje široká veřejnost, a tím výrazně zasahuje do soukromí velkého počtu osob. Podobně na tom bude také kamera číslo

2 směřující na okna a kamera číslo 11 umístěná ve venkovním prostoru, která by mohla snímat osoby ze sousedních budov. Hodnocení ostatních kamer je rovněž velmi vysoké, jelikož se jedná o kamery zachycující identitu jednotlivých osob a po budově školy se může pohybovat velké množství osob (kromě studentů a učitelů to mohou být také rodiče a návštěvy školy).

Hodnocení kamer v poslední kategorii je rovněž vysoké, a to hlavně díky velkému počtu osob, jejichž osobní údaje jsou zpracovávány. Kamery snímající dveře kanceláří mají o něco nižší hodnocení, kvůli omezení doby nahrávání. Hodnocení také snižuje nastavení režimu kamer pro nahrávání pouze při detekci pohybu. Především u kamery číslo 1 však lze předpokládat, že bude nahrávat velmi často.

Při porovnání tabulky 5.4 s tabulkou 5.3 může být na základě výsledného hodnocení jednotlivých kamer stanovena jejich rizikovost. Je možné vidět, že výsledné hodnocení kamer se pohybuje v rozmezí od -3 do -6.

U kamer číslo 3, 7, 9 a 10 lze na základě jejich výsledného hodnocení konstatovat, že představují nízké riziko pro zásah do soukromí subjektů údajů. Přesto by u nich měl být zvýšen stupeň zabezpečení a zváženy další možné dopady kamer.

Ostatní kamery jsou hodnoceny hůře a představují střední riziko pro soukromí subjektů údajů. U těchto kamer je nutné přijmout nápravná opatření. Základním opatřením by mělo být zvýšení jejich zabezpečení. Dále je nutné promyslet změnu nastavení kamer, úhel jejich záběrů a případné přidání privátních masek.

5.6 Návrhy opatření pro soulad kamerového systému s GDPR

Na základě provedených analýz spojených s plánovaným zavedením kamerového systému ve škole BMA bylo navrženo několik nezbytných opatření, která je nutné aplikovat pro soulad kamerového systému s požadavky Obecného nařízení.

Prvním navrhovaným krokem, který by měl být zvážen již při provádění rekonstrukce školy, je vybudování samostatné uzamykatelné místnosti pro datový rozvaděč. Klíč od této místnosti by měly mít pouze některé pověřené osoby, což povede ke zvýšení fyzického zabezpečení dat. Toto opatření bude mít rovněž pozitivní vliv na výsledek analýzy DPIA.

Dalším krokem, který bude pro správný provoz kamerového systému nezbytný, je pověření osoby odpovědné za provoz tohoto systému a určení, které osoby budou mít

právo přístupu k živému obrazu z kamer, což budou například pracovníci sekretariátu z důvodu kontroly vstupu do budovy. Společně s tím je nutné stanovit osoby, které budou mít právo na přístup ke kamerovým záznamům.

Následně musí být zajištěna tvorba interní směrnice pro kamerový systém, ve které budou jasně stanovena pravidla jeho provozu, uvedena osoba odpovědná za provoz systému a osoby s právem přístupu ke kamerovým záznamům.

Na vstupních dveřích do budovy by měla být vylepena informační cedule o provozování kamerového systému se záznamem. Tato cedule musí obsahovat především informaci, že v prostorách budovy je provozován kamerový systém se záznamem a doporučuje se přidat také obrázek kamery, aby byla informace snáze pochopitelná a více poutala pozornost. Dále by na ceduli měly být uvedeny informace o správci a kontakt na odpovědnou osobu.

U kamery číslo 1 umístěné u hlavního vchodu do budovy by měl být obraz nastaven tak, aby kamera nezachycovala dění venku za prosklenými dveřmi. V případě, že by takovéto nastavení kamery nebylo možné, bude nutné opatřit obraz z kamery takzvanou privátní zónou pro zakrytí nevhodné části tohoto obrazu.

Zvláštní opatření bude nutné také u kamery číslo 11 umístěné na venkovní terase. Při umisťování této kamery bude muset být ověřeno, zda obraz nezaznamenává okolní budovy. Jestliže tomu tak bude, je nutné využít privátní zónu pro zakrytí všech oken okolních budov.

Dále bude důležité zvážit dobu nezbytnou pro uchovávání kamerových záznamů. S ohledem na negativní hodnocení kamer v rámci analýzy DPIA je zkrácení doby uchovávání záznamů jednou z cest, jak toto negativní hodnocení vylepšit.

Posledním nezbytným krokem pro dodržení souladu s GDPR je doplnění zpracování osobních údajů kamerovým systémem do karty záznamů o činnostech zpracování, a to včetně všech potřebných informací. Dobré je také doplnit odkaz na interní směrnici a analýzu DPIA pro snadné dohledání podrobností v případě auditu.

6 Závěr

Diplomová práce byla vypracována na základě požadavku soukromé školy o vypracování návrhu projektu pro zavedení kamerového systému splňujícího požadavky Obecného nařízení GDPR.

Hlavním cílem této diplomové práce bylo navržení nezbytných kroků správné implementace požadavků GDPR spojených se zavedením kamerového systému ve škole Gymnázium BESKYDY MOUNTAIN ACADEMY, s.r.o. V souvislosti s tímto cílem bylo nutné nejprve zmapovat prostředí organizace a navrhnout hlavní kroky implementace GDPR vyplývající z Obecného nařízení, což bylo provedeno ve čtvrté kapitole. Prvním krokem praktické části práce bylo vypracování studie proveditelnosti pro projekt implementace GDPR spojeného se zavedením kamerového systému v dané instituci. Součástí studie byl popis projektu, včetně jeho technického řešení a odhadu vynaložených nákladů v případě jeho realizace. Dále byla zpracována hierarchická struktura prací projektu, včetně jeho časového odhadu. Kvůli zajištění souladu s GDPR byla provedená zkrácená GAP analýza zaměřující se na požadavky GDPR u kamerových systémů. Následně byl vypracován návrh kamerového systému, který byl nezbytný pro DPIA analýzu. V poslední části byly navrženy všechny nezbytné kroky a opatření pro soulad kamerového systému s požadavky GDPR. K realizaci projektu by mělo dojít v následujících dvou letech a dá se předpokládat, že do ní bude zapojen také odborník na GDPR a kamerové systémy, s nímž byla práce konzultována.

Dílčím cílem práce bylo navržení obecných kroků prvotní implementace požadavků GDPR ve školských organizacích, které se doposud tímto problémem nezabývaly. Tento cíl byl navržen za účelem usnadnění celkové implementace GDPR ve školách. Pro splnění tohoto cíle byla nejprve vypracována tabulka WBS obsahující všechny základní kroky úspěšné implementace. Následně byla řešena problematika analyzování procesů zpracování osobních údajů ve školách a současně byla vypracována vzorová karta záznamů o zpracování osobních údajů. V tomto dokumentu jsou navrženy základní účely zpracování osobních údajů, k nimž ve školách dochází, a také obsahuje upřesnění nezbytných informací, které musí být v souvislosti se zpracováním osobních údajů zaznamenávány. V dalším kroku byla přehledně navržena a popsána tabulka pro GAP analýzu, včetně zmapování nejnutnějších požadavků GDPR, na které je důležité se v každé organizaci zaměřit. V posledním kroku, souvisejícím s tímto cílem práce, byla navržena a vysvětlena metodika DPIA využitelná především pro případ provozování kamerových systémů ve školách. Závěrem lze konstatovat, že všechny stanovené cíle této diplomové práce byly splněny.

Seznam použité literatury

Knižní zdroje

BENDOVÁ, Klára a kol. *Základy projektového řízení.* 1. vyd. Olomouc: Univerzita Palackého, 2012. ISBN 978-80-244-3124-6.

DOLEŽAL, Jan. *Projektový management: komplexně, prakticky a podle světových standardů.* Praha: Grada Publishing, 2016. ISBN 9788024756202.

DOLEŽAL, Jan a Jiří KRÁTKÝ. *Projektový management v praxi: naučte se řídit projekty!*. Praha: Grada, 2017. ISBN 978-80-247-5693-6.

FIALA, Petr. *Projektové řízení: modely, metody, analýzy*. Praha: Professional Publishing, 2004. ISBN 80-86419-24-X.

NEZMAR, Luděk. *GDPR: praktický průvodce implementací.* Praha: Grada Publishing, 2017. Právo pro praxi. ISBN 978-80-271-0668-4.

NĚMEC, Vladimír. *Projektový management*. Praha: Grada, 2002. ISBN 80-2470-392-0.

NONNEMANN, František. *Příručka pověřence pro ochranu osobních údajů*. Praha: Nakladatelství Klika, 2018. ISBN 978-80-88298-10-6.

NULÍČEK, Michal a kol. *GDPR – Obecné nařízení o ochraně osobních údajů.* 2. vydání. Praha: Wolters Kluwer, 2018. ISBN 978-80-7598-068-7.

Project Management Institue. *A guide to the project management body of knowledge (PMBOK guide).* Fifth edition. Newtown Square, Pennsylvania: Project Management Institute, 2013. ISBN 978-1-935589-67-9.

ROSENAU, Milton D. *Řízení projektů*. Vyd. 3. Brno: Computer Press, 2007. Business books. ISBN 978-80-251-1506-0.

ŘEHÁČEK, Petr. *Projektové řízení podle PMI*. Praha: Ekopress, 2013. ISBN 978-80-86929-90-3.

SCHWALBE, Kathy. *Řízení projektů v IT: kompletní průvodce.* 1. vyd. Brno: Computer Press, 2011. ISBN 978-80-251-2882-4.

SVOZILOVÁ, Alena. *Projektový management: systémový přístup k řízení projektů*. 3. aktualizované a rozšířené vydání. Praha: Grada Publishing, 2016. ISBN 978-80-271-0075-0.

VOKÁL, Zdeněk a Radim Štork. *Projektový management.* Praha: Vyšší odborná škola sociálně právní, 2013. ISBN 978-80-87779-08-8.

ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG). ISBN 978-80-7554-152-9.

Elektronické zdroje

BESTPRACTICE.CZ. *Projektové řízení & PRINCE2* [online]. © 2019 [cit. 2019-02-28]. Dostupné z: https://www.bestpractice.cz/cs/Best-practice/PM-PRINCE2-.alej

ČESKÁ KOMORA PMI. *Certifikace – Česká komora PMI* [online]. Copyright © 2019 Česká komora PMI [cit. 2019-03-03]. Dostupné z: https://www.pmi.cz/index.php/cs/professional-development/50.html

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *Studie proveditelnosti – osnova* [online]. © 2019 [cit. 2019-02-24]. Dostupné z: http://www.mvcr.cz/soubor/osnova-studie-proveditelnosti-pdf.aspx

Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (Obecné nařízení o ochraně osobních údajů). In: *Úřední věstník Evropské unie* [online]. [cit. 2019-02-28] Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=32394

SIEBER, Patrik. *Studie proveditelnosti (Feasibility Study) metodická příručka* [online]. Ministerstvo pro místní rozvoj, © 2004 [cit. 2019-02-24]. Dostupné z: https://www.dotaceeu.cz/getmedia/c4772855-8ffc-4036-97fc-2d7caa1ad86e/1136372156-zpracov-n-studie-proveditelnosti

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Základní příručka k GDPR* [online]. © 2017 ÚOOÚ [cit. 2019-02-09]. Dostupné z: https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/p1=4744

Seznam zkratek

BMA	Beskydy Mountain Academy
CPM	Critical Path Method
CRAMM	CCTA Risk Analysis and Management Method
DPH	Daň z přidané hodnoty
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EU	Evropská unie
FMEA	Failure Mode and Effect Analysis
GDPR	General Data Protection Regulation
HACCP	Hazard Analysis and Critical Control Points
HW	Hardware
ICB	IPMA Competence Baseline
IT	Informační technologie
IPMA	International Project Management Association
ISMS	Information Security Management System
ISO	International Standards Organization
MS	Microsoft
MŠMT	Ministerstvo školství, mládeže a tělovýchovy České republiky.
OÚ	Osobní údaje
PM BoK	Project Management Body of Knowledge
PMI	Project Management Institute
PRINCE	Project IN Controlled Environments
SMART	Specific, Measurable, Achievable, Realistic, Time-oriented
SW	Software
SWOT	Strengths, Weaknesses, Opportunities, Threats
WBS	Work Breakdown Structure

Seznam obrázků

Seznam tabulek

Prohlašuji, že

- jsem byla seznámena s tím, že na mou diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. – autorský zákon, zejména § 35 – užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního a § 60 – školní dílo;
- beru na vědomí, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen VŠB-TUO) má právo nevýdělečně, ke své vnitřní potřebě, bakalářskou práci užít (§ 35 odst. 3);
- souhlasím s tím, že diplomová práce bude v elektronické podobě archivována v Ústřední knihovně VŠB-TUO. Souhlasím s tím, že bibliografické údaje o diplomové práci budou zveřejněny v informačním systému VŠB-TUO;
- bylo sjednáno, že s VŠB-TUO, v případě zájmu z její strany, uzavřu licenční smlouvu s oprávněním užít dílo v rozsahu § 12 odst. 4 autorského zákona;
- bylo sjednáno, že užít své dílo, diplomovou práci, nebo poskytnout licenci k jejímu využití mohu jen se souhlasem VŠB-TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB-TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).

V Ostravě dne 23. 4. 2019

Vaňková

……

Bc. Anna Vaňková

Seznam příloh